MN128-SOHO

IB3

活用ガイド～中・上級編

■商標についてのお知らせ

◎ Microsoft®、Windows®は、米国Microsoft® Corporationの登録商標です。
◎ Macintosh®、Mac®、MacOS®は、アップルコンピュータ社の登録商標です。
◎ Ethernet®は、富士ゼロックス社の登録商標です。
◎ Super G™は、Atheros Communications, Inc.の商標です。
◎ Adobe、Acrobat、Readerは、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における登録商標または商標です。
◎ MN128SOHO™は、株式会社エヌ・ティ・ティ エムイーの商標です。
◎ AutoBACP™、AutoDNS™、AutoMP™、AutoNAT™、AutoPAD™、AutoPPP™、マルチアンサー™は、株式会社ビー・ユー・ジーの商標です。
◎ その他の商品名、会社名は、各社の商標または登録商標です。

■ご注意

- この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置を家庭環境で使用すると電波障害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。取扱説明書に従って正しい取り扱いをしてください。
- 本製品の故障、誤動作、不具合あるいは停電などの外的要因によって、通信などの機会を逃したために生じた損害などの純粋経済損失につきましては、当社は一切その責任を負いかねますので、あらかじめご了承ください。
- 通信不良によって生じた損害につきましては、当社は一切その責任を負いかねますので、あらかじめご了承ください。また、通信内容の漏れにつきましても、当社は一切その責任を負いかねますので、あらかじめご了承ください。
- このマニュアルの著作権は、すべて株式会社エヌ・ティ・ティ エムイーに帰属します。
- このマニュアルの内容の一部または全部を無断で転用することは禁止されています。
- このマニュアルおよびソフトウェア、ハードウェア、外観の内容について、将来予告なしに変更することがあります。

もくじ

9 コールバック接続する

10 リモートアクセスサーバ

11 その他の接続方法

12 保守

付録

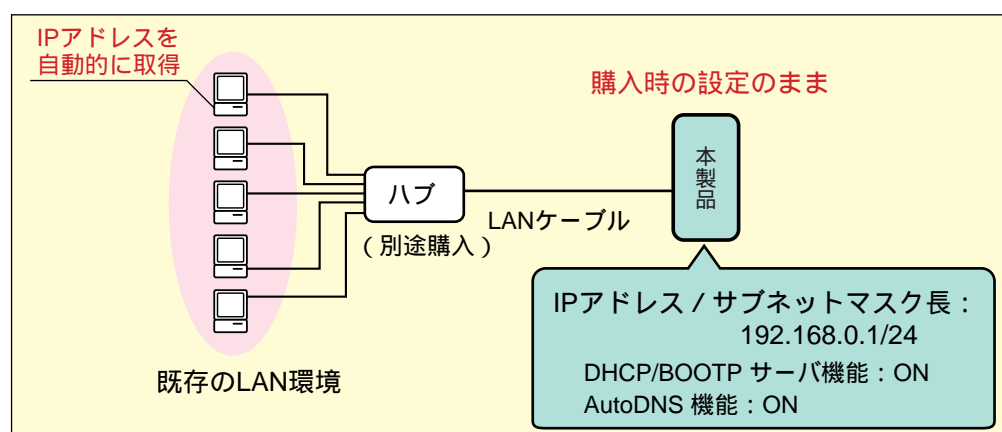
活用ガイド

中・上級編

中上級編では、コンピュータやネットワークについての知識をお持ちの方、初級編の内容を理解している方を対象に、次の事項を解説します。

1 LANの環境を整える

既存のLAN環境で使用する
（1）購入時のIPアドレスのまま導入する

本製品のIPアドレスを、購入時のままでLANに導入する場合について解説します。この場合、本製品の設定ページを開くには、LAN側のパソコンのIPアドレス（サブネットワークアドレス）を本製品にあわせる必要があります。

本製品の購入時の設定は次のとおりです。

本体のIPアドレス/サブネットマスク長	192.168.0.1/24
DHCPサーバ機能	ON
AutoDNS機能	ON

上記の設定のままLANで利用するには、LAN側のサブネットワークアドレスを「192.168.0.X/24」に設定し、本製品と同じサブネットワークにする必要があります。

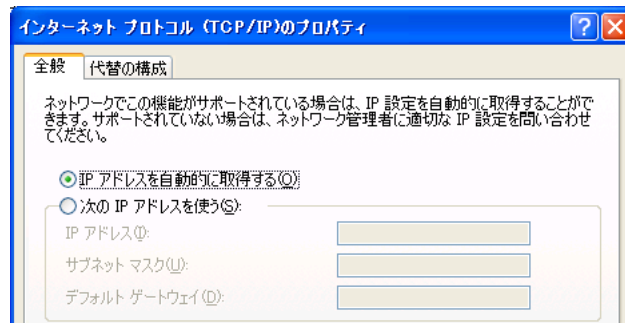
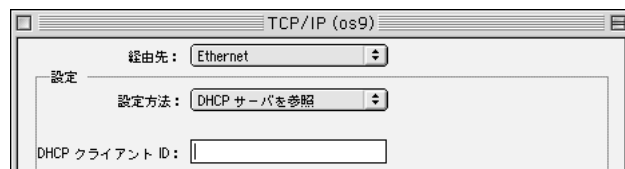
パソコン側のIPアドレスを設定する方法はいくつかありますが、ここでは、本製品のDHCP/BOOTPサーバ機能を使用して、本製品からIPアドレスを自動的に取得する方法を例にして解説します。

パソコンの設定

■IPアドレスをDHCPサーバから自動的に取得します

1. IPアドレスを自動的に取得するように設定します。次のダイアログで設定します。

Windows XP	：［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティ］
Windows 2000	：［コントロールパネル］→［ネットワークとダイヤルアップ接続］→［ローカルエリア接続］のプロパティ
Windows 98 SE/Me	：［コントロールパネル］→［ネットワーク］
Macintosh	：［コントロールパネル］→［TCP/IP］

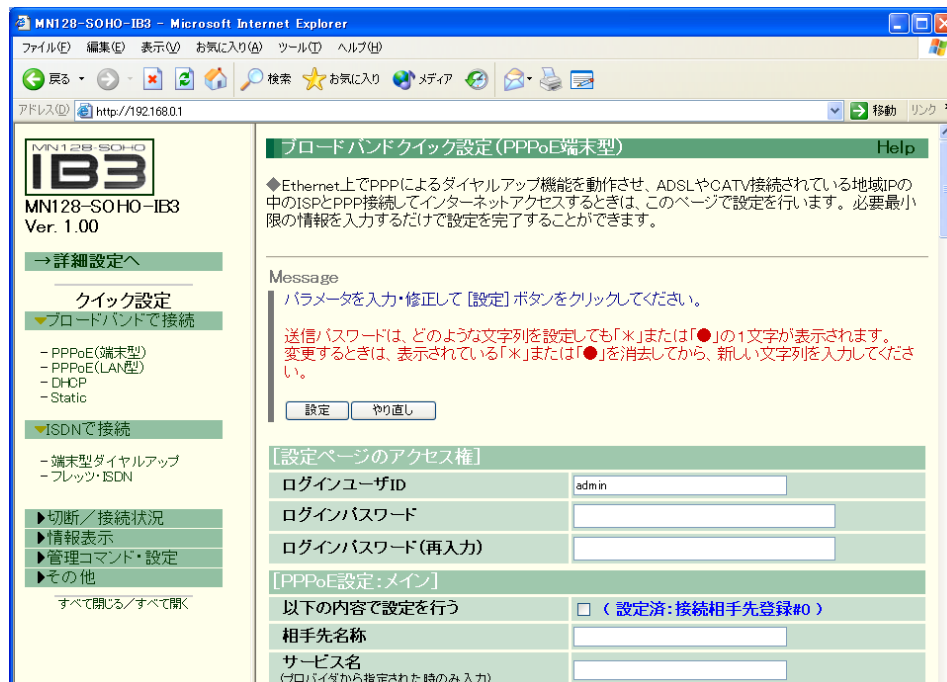
（例）Windows XPの場合

（例）Macintoshの場合

2. パソコンを再起動します。

   再起動後、本製品からIPアドレスを自動的に取得できます。

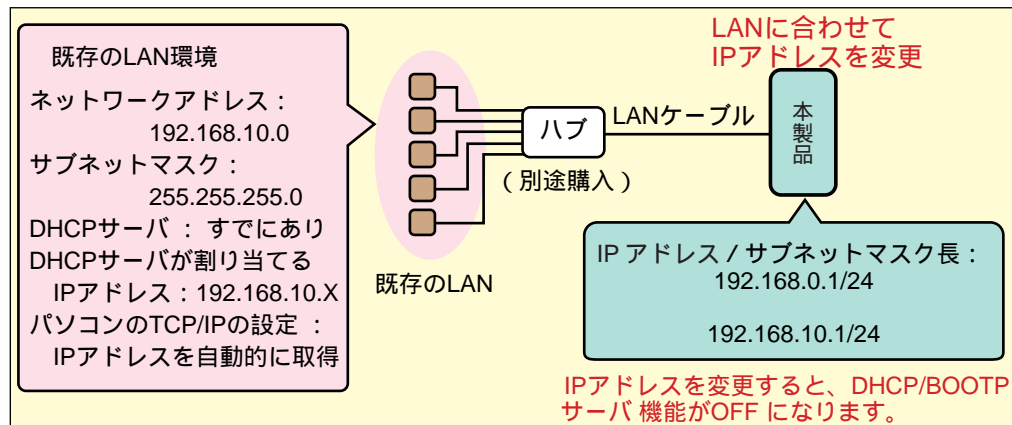
この操作の前に、別のDHCPサーバからIPアドレスを取得していた場合、リース時間が経過するまで、前のIPアドレスを使用し続けます。この場合、「IPアドレスの再取得方法について」〈P.17〉を参照して、IPアドレスを更新してください。なお、IPアドレスを取得できるパソコンは、購入時の設定では32台までです。

操作

■設定ページを開きます

1. Webブラウザを起動して、［URL］の欄に「http://192.168.0.1/」と入力します。

以降、このページで、ルータ機能の設定を行うことができます。

既存のLAN環境で使用する
（2）本製品のIPアドレスを変更して導入する

LANの環境に合わせて本製品のIPアドレスを変更してから、LANに導入する場合について解説します。ここでは、TELポートにつないだ電話機から、IPアドレスを変更します。

設定

■本製品のIPアドレスを変更します。

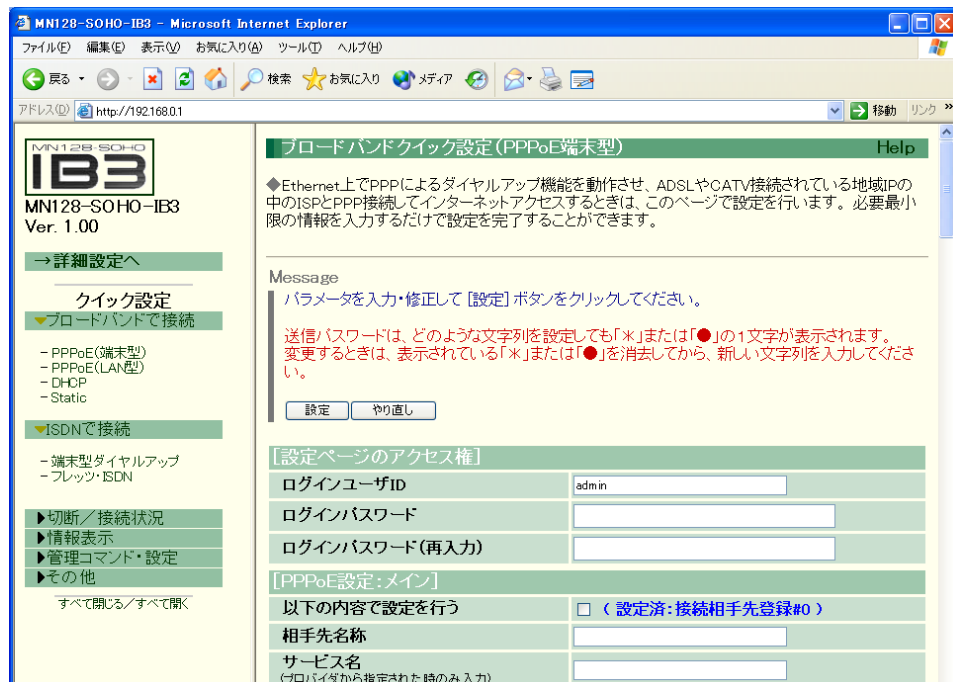
TELポートの電話機から設定コード（#1）を使って、本製品のIPアドレスを変更します。

1. TELポートの電話機の受話器を上げ、「ツー」という音を確認します。
2. フックを1回押すと、「プッップッ」と聞こえます。
3. ［#］ボタンを押すと、無音になります。
4. ［1］ボタンを押すと、「ピッピッピッ」と聞こえ、設定モードになります。
5. ［#］［1］ボタンを押すと、「ピッ」と聞こえます。
6. 続けて、次の要領でボタンを押して、本製品のIPアドレスを設定します。
   ※IPアドレスの「.（ドット）」の代わりに［#］ボタンを押します。IPアドレスとサブネットマスク長の区切りにも［#］を押します。
   192［#］168［#］10［#］1［#］24
7. ［#］ボタンを押すと、「ピーッ」と聞こえます。
8. 設定が終了したので、受話器を置きます。
9. 本製品を再起動します。

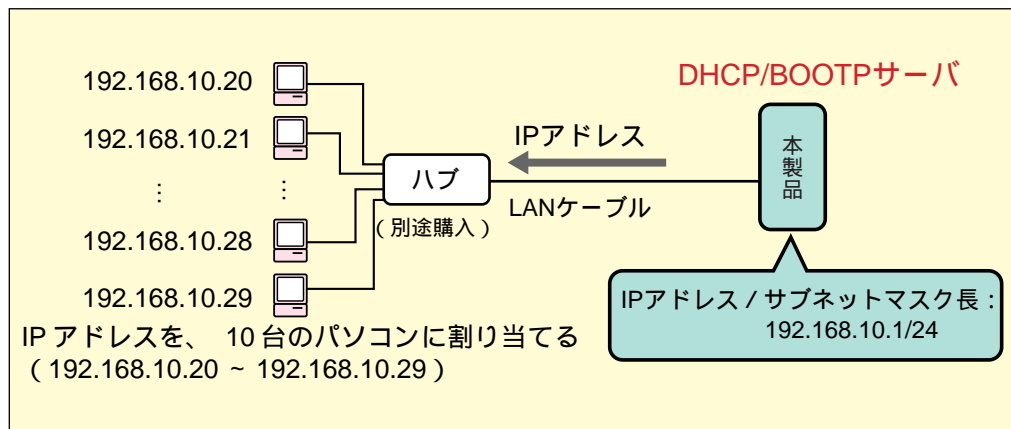
本製品のIPアドレスを変更すると、DHCP/BOOTPサーバ機能がOFFになります。

操作

■設定ページを開きます

1. Webブラウザを起動して、［URL］の欄に「http://192.168.10.1/」と入力します。

以降、このページで、ルータ機能の設定を行うことができます。

DHCP/BOOTPサーバ機能を使う

DHCP/BOOTPサーバ機能を使用するときは、設定ページでDHCP/BOOTPサーバ機能をONにします。

LAN内にほかのDHCPサーバがある場合は、本製品のDHCP/BOOTPサーバ機能をONにしないでください。

設定ページ

■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス／サブネットマスク長	192.168.10.1/24 ※すでに固定のIPアドレスが割り当てられたパソコンがある場合は、そのIPアドレス以外のIPアドレスを割り当ててください。
DHCPサーバ機能	ONを選択
開始IPアドレス/個数	192.168.10.20/10 ※割り当てるIPアドレスのうち、最初のIPアドレスと、割り当てるIPアドレスの個数を入力します。 ※すでに固定のIPアドレスが割り当てられたパソコンがある場合は、そのIPアドレス以外のIPアドレスを割り当ててください。

パソコンの設定

■パソコンのTCP/IPの設定を変更して、IPアドレスを自動的に取得します。

1. IPアドレスを自動的に取得するように設定します。次のダイアログで設定します。

Windows XP　：［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティ］
Windows 2000　：［コントロールパネル］→［ネットワークとダイヤルアップ接続］→［ローカルエリア接続］のプロパティ
Windows 98 SE/Me：［コントロールパネル］→［ネットワーク］
Macintosh　：［コントロールパネル］→［TCP/IP］

2. パソコンを再起動します。

再起動後、本製品からIPアドレスを自動的に取得できます。
※取得したIPアドレスを確認する方法は、「IPアドレスの再取得方法について」〈P.17〉を参照してください。

この操作の前に、別のDHCPサーバからIPアドレスを取得していた場合、リース時間が経過するまで、前のIPアドレスを使用し続けます。この場合、「IPアドレスの再取得方法について」〈P.17〉を参照して、IPアドレスを更新してください。

◆設定されたIPアドレスを確認したいときは
DHCPサーバ機能によって自動で設定されたIPアドレスは、次の方法で確認できます。

（1）Windowsの場合
MS-DOSプロンプトまたはコマンドプロンプトで確認することができます。詳しくは、「IPアドレスの再取得方法について」〈P.17〉を参照してください。

（2）Macintoshの場合
［コントロールパネル］→［TCP/IP］で確認することができます。

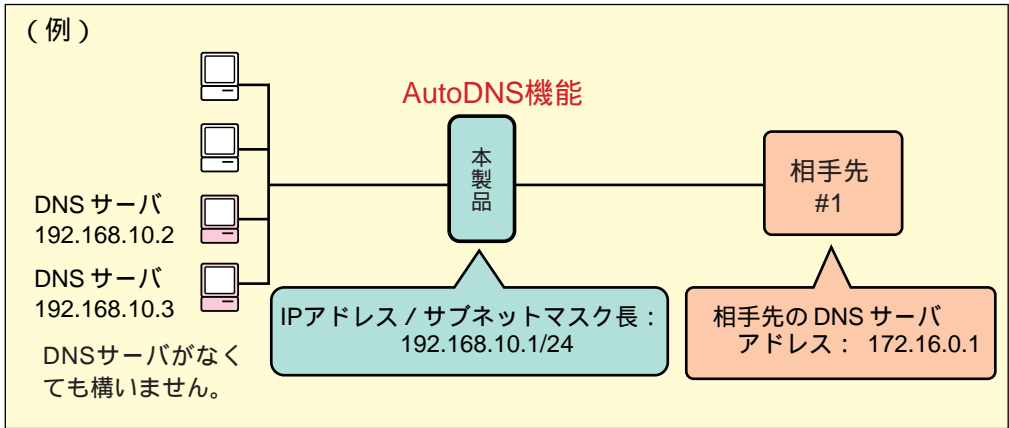
なお、IPアドレスは、パソコンを起動後、最初にWebブラウザなどのTCP/IPを使うアプリケーションを起動したときに設定されます。

◆DHCP/BOOTPサーバ機能を使用しないときは
本製品のDHCP/BOOTPサーバ機能をOFFにしたときは、次の点に注意してパソコンのIPアドレスを設定し直してください。

- 本製品と同じサブネットのIPアドレスを設定すること
- 本製品やLAN上のほかの端末（パソコンなど）のIPアドレスと重複しないように設定すること

◆IPアドレスとパソコンの組み合わせを固定にすることもできます
DHCP/BOOTPサーバ機能を使ってパソコンのIPアドレスを設定する際、パソコンと設定するIPアドレスの組み合わせを固定できます。「DHCP/BOOTPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定する」〈P.24〉を参照してください。

AutoDNS機能を使う

本製品のAutoDNS機能を使用すると、接続する相手先を変更したときでも、パソコンのDNSサーバのIPアドレスを設定し直す必要がなくなります。なお、購入時はAutoDNS機能はONです。

設定ページ

■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス/サブネットマス	192.168.10.1/24
AutoDNS機能	ON を選択
LAN 側 DNS サーバアドレス（プライマリ）/ LAN 側 DNS サーバアドレス（セカンダリ）	LAN 側の DNS サーバを常に優先して使いたいとき、これらの項目にその DNS サーバの IP アドレスを入力します。 192.168.10.2 192.168.10.3 ※ LAN 側に DNS サーバがなくても本機能が使えます。 LAN 側に DNS サーバがないときは、空白にしてください。

■［詳細設定］→［接続／相手先登録］→［＃1］

DNS サーバアドレス	172.16.0.1

パソコンの設定

■パソコンのTCP/IPの設定を変更します。

各OSのTCP/IP設定の画面で、次のように設定します。

●Windows XPの場合（[コントロールパネル] → [ネットワークとインターネット接続] → [ネットワーク接続] → [ローカルエリア接続] のプロパティ）

本製品の DHCP サーバ機能が ON のとき	
[全般] タブ	[DNS サーバーのアドレスを自動的に取得する] を選択
本製品の DHCP サーバ機能が OFF のとき	
[全般] タブ	[次の DNS サーバーのアドレスを使う] を選択し、次の項目を設定 [優先 DNS サーバー] →本製品の IP アドレスを入力

●Windows 2000の場合（[コントロールパネル] → [ネットワーク接続] → [ローカルエリア接続] のプロパティ）

本製品の DHCP サーバ機能が ON のとき	
[全般] タブ	[DNS サーバーのアドレスを自動的に取得する] を選択
本製品の DHCP サーバ機能が OFF のとき	
[全般] タブ	[次の DNS サーバーのアドレスを使う] を選択し、次の項目を設定 [優先 DNS サーバー] →本製品の IP アドレスを入力

●Windows 98 SE/Meの場合（[コントロールパネル] → [ネットワーク]）

本製品の DHCP サーバ機能が ON のとき	
[DNS 設定] タブ	[DNS を使わない] を選択
[ゲートウェイ] タブ	[インストールされているゲートウェイ] からすべての IP アドレスを削除
本製品の DHCP サーバ機能が OFF のとき	
[DNS 設定] タブ	[DNS を使う] を選択し、次の項目を設定 ホスト → パソコンに付ける名前を入力 DNS サーバの検索順 → 本製品の IP アドレスを入力
[ゲートウェイ] タブ	本製品または同一サブネット上のゲートウェイ（ルータ）の IP アドレスを入力

●Macintoshの場合（[コントロールパネル] → [TCP/IP] → [ローカルエリア接続] のプロパティ）

本製品の DHCP サーバ機能が ON のとき	
何も設定しません。（[DHCP サーバを参照] を選択するだけです。） ※ MacOS のバージョンによっては、[ネームサーバアドレス] に本製品の IP アドレスを入力する必要があります。	
本製品の DHCP サーバ機能が OFF のとき	
ルータアドレス	本製品または同一サブネット上のゲートウェイ（ルータ）の IP アドレスを入力
ネームサーバアドレス	本製品の IP アドレスを入力

この操作を行っても通信できないときは、下記の「AutoDNS機能を使用しないときは」に従って操作してください。

◆AutoDNS機能を使用しないときは

本製品のAutoDNS機能をOFFにしたときは、パソコンのTCP/IPを次のように設定します。

● Windows XPの場合（[コントロールパネル] → [ネットワークとインターネット接続] → [ネットワーク接続] → [ローカルエリア接続] のプロパティ）

本製品のDHCPサーバ機能がON、かつ、LAN側DNSサーバアドレスを設定しているとき	
[全般] タブ	[DNS サーバのアドレスを自動的に取得する] を選択
上記以外のとき	
[全般] タブ	[次の DNS サーバーのアドレスを使う] を選択し、次の項目を設定 [優先 DNS サーバー] [代替 DNS サーバー] →使用する DNS サーバの IP アドレスを入力

● Windows 2000の場合（[コントロールパネル] → [ネットワーク接続] → [ローカルエリア接続] のプロパティ）

本製品のDHCPサーバ機能がON、かつ、LAN側DNSサーバアドレスを設定しているとき	
[全般] タブ	[DNS サーバのアドレスを自動的に取得する] を選択
上記以外のとき	
[全般] タブ	[次の DNS サーバーのアドレスを使う] を選択し、次の項目を設定 [優先 DNS サーバー] [代替 DNS サーバー] →使用する DNS サーバの IP アドレスを入力

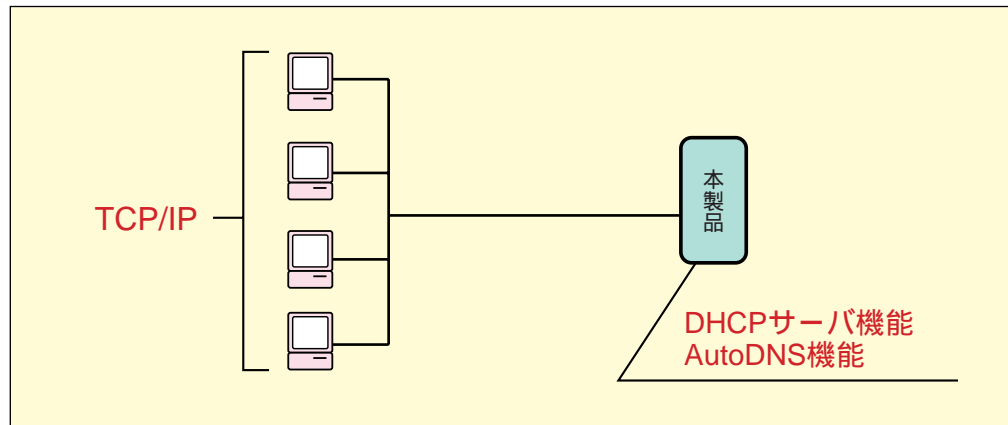
● Windows 98 SE/Meの場合（[コントロールパネル］→［ネットワーク]）

本製品のDHCPサーバ機能がON、かつ、LAN側DNSサーバアドレスを設定しているとき	
［全般］タブ	［DNS サーバのアドレスを自動的に取得する］を選択
上記以外のとき	
［全般］タブ	［次の DNS サーバーのアドレスを使う］を選択し、次の項目を設定 ［優先 DNS サーバー］［代替 DNS サーバー］ →使用する DNS サーバの IP アドレスを入力

●Macintoshの場合（[コントロールパネル］→［TCP/IP］→［ローカルエリア接続］のプロパティ）

本製品のDHCPサーバ機能がON、かつ、LAN側DNSサーバのアドレスを設定しているとき	
何も設定しません。（［DHCPサーバを参照］を選択するだけです。） ※MacOSのバージョンによっては、［ネームサーバアドレス］に、使用するDNSサーバのIP アドレスを入力する必要があります。	
上記以外のとき	
ルータアドレス	本製品または同一サブネット上のゲートウェイ（ルータ）のIPアドレスを入力
ネームサーバアドレス	使用する DNS サーバの IP アドレスを入力 （プロバイダから指定されている DNS サーバの IP アドレスなど）
追加の検索ドメイン	使用するドメイン名を入力

IPアドレスの再取得方法について

一度DHCPサーバからIPアドレスを取得した場合、IPアドレスを変更しても、IPアドレスのリース期間が経過するまでは自動的に更新されません。更新するための操作方法について解説します。

設定

●Windows XPの場合

1. ［スタート］ボタン→［コントロールパネル］を選択します。
2. ［ネットワークとインターネット接続］→［ネットワーク接続］を選択します。次に［ローカルエリア接続］を右クリックし、［状態］を選択します。
   ［ローカルエリアネットワークの状態］ダイアログが表示されます。
3. ［サポート］タブをクリックし、［修復］ボタンをクリックします。
   以前取得したIPアドレスが無効になり、新しいIPアドレスが設定されます。

●Windows 2000の場合

1. ［スタート］ボタン→［プログラム］→［アクセサリ］→［コマンドプロンプト］をクリックします。
   ［コマンドプロンプト］ウィンドウが表示されます。
2. 「ipconfig/release」と入力し、［Enter］キーを押します。
   以前取得したIPアドレスは無効になります。
3. 「ipconfig/renew」と入力し、［Enter］キーを押します。
   新しいIPアドレスが設定されます。

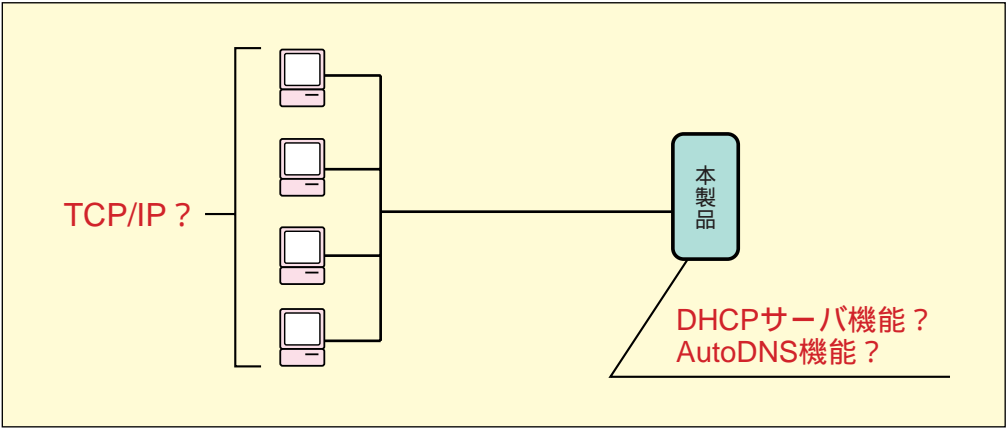
●Windows 98 SE/Meの場合

1. ［スタート］ボタン→［プログラム］→［MS-DOSプロンプト］をクリックします。
   ［MS-DOSプロンプト］ウィンドウが表示されます。
2. 「winipcfg」と入力し、［Enter］キーを押します。
   ［IP設定］ダイアログが表示されます。
3. 使用しているEthernetボードを選択し、［解放］ボタンをクリックします。
   ［IPアドレス］が「0.0.0.0」に変わり、以前取得したIPアドレスは無効になります。
4. ［書き換え］ボタンをクリックします。
   新しいIPアドレスが設定されます。

●Macintoshの場合

パソコンを再起動すると、IPアドレスが更新されます。

TCP/IP設定早見表

本製品のDHCPサーバ機能とAutoDNS機能の設定に対する、パソコンのTCP/IPの設定内容をまとめると、次のようになります。

設定

●Windows XPの場合

		AutoDNS 機能 ON	AutoDNS 機能 OFF
DHCPサーバ機能	ON	●IP アドレス ［IP アドレスを自動的に取得する］を選択 ●DNS ［DNS サーバーのアドレスを自動的に取得する］を選択	●IP アドレス ［IP アドレスを自動的に取得する］を選択 ●DNS ［DNS サーバーのアドレスを自動的に取得する］を選択 ☞「DNS の設定について」〈P.21〉を参照
DHCPサーバ機能	OFF	●IP アドレス ［次の IP アドレスを使う］を選択し、IP アドレス・サブネットマスクを入力、［デフォルトゲートウェイ］に本製品の IP アドレスを入力 ●DNS ［次の DNS サーバーのアドレスを使う］を選択し、［優先 DNS サーバー］に、本製品の IP アドレスを入力	●IP アドレス ［次の IP アドレスを使う］を選択し、IP アドレス・サブネットマスクを入力、［デフォルトゲートウェイ］に本製品の IP アドレスを入力 ●DNS ［次の DNS サーバーのアドレスを使う］を選択し、［優先 DNS サーバー］に、使用する DNS サーバの IP アドレスを入力

●Windows 2000の場合

		AutoDNS 機能	
		ON	OFF
DHCPサーバ機能	ON	●IP アドレス ［IP アドレスを自動的に取得する］を選択 ●DNS ［DNS サーバーのアドレスを自動的に取得する］を選択	●IP アドレス ［IP アドレスを自動的に取得する］を選択 ●DNS ［DNS サーバーのアドレスを自動的に取得する］を選択 ☞「DNS の設定について」〈P.21〉を参照
	OFF	●IP アドレス ［次の IP アドレスを使う］を選択し、IP アドレス・サブネットマスクを入力、［デフォルトゲートウェイ］に本製品の IP アドレスを入力 ●DNS ［次の DNS サーバーのアドレスを使う］を選択し、［優先 DNS サーバー］に、本製品の IP アドレスを入力	●IP アドレス ［次の IP アドレスを使う］を選択し、IP アドレス・サブネットマスクを入力、［デフォルトゲートウェイ］に本製品の IP アドレスを入力 ●DNS ［次の DNS サーバーのアドレスを使う］を選択し、［優先 DNS サーバー］に、使用する DNS サーバの IP アドレスを入力

●Windows 98 SE/Meの場合

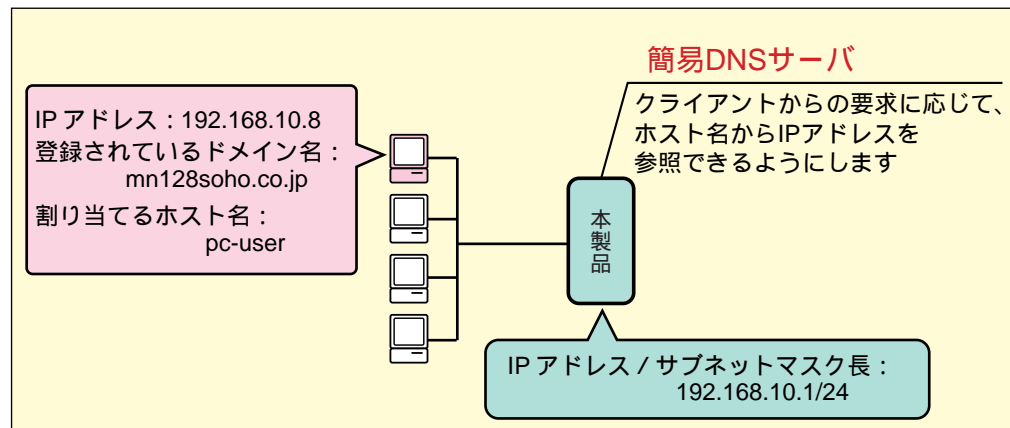
		AutoDNS 機能	
		ON	OFF
DHCPサーバ機能	ON	●IP アドレス ［IPアドレスを自動的に取得］を選択 ●DNS 設定 ［DNS を使わない］を選択	●IP アドレス ［IP アドレスを自動的に取得］を選択 ●DNS 設定 ［DNS を使わない］を選択 ☞「DNS の設定について」〈P.21〉を参照
	OFF	●IP アドレス ［IP アドレスを指定］を選択し、IP アドレス、サブネットマスクを入力 ●DNS 設定 ［DNS を使う］を選択し、［ホスト］にパソコンに付ける名前を、［ドメイン名］に使用するドメイン名を、［DNS サーバの検索順］に本製品の IP アドレスを入力 ●ゲートウェイ 本製品または同一ネット上のゲートウェイ（ルータ）の IP アドレスを入力	●IP アドレス ［IP アドレスを指定］を選択（IP アドレス・サブネットマスクを入力） ●DNS 設定 ［DNS を使う］を選択し、［ホスト］にパソコンに付ける名前を、［ドメイン名］に使用するドメイン名を、［DNS サーバの検索順］に使用する DNS サーバの IP アドレスを入力 ●ゲートウェイ 本製品または同一ネット上のゲートウェイ（ルータ）の IP アドレスを入力

●Macintoshの場合

		AutoDNS 機能	
		ON	OFF
DHCPサーバ機能	ON	●設定方法 ［DHCP サーバを参照］を選択 ※ MacOS のバージョンによっては、［ネームサーバアドレス］に、本製品の IP アドレスを入力する必要があります。	●設定方法 ［DHCP サーバを参照］を選択 ※ MacOS のバージョンによっては、［ネームサーバアドレス］に、使用する DNS サーバの IP アドレスを入力する必要があります。 ☞下記の「DNS の設定について」を参照
	OFF	●設定方法 ［手入力］を選択（IP アドレス・サブネットマスクを入力） ●ルータアドレス 本製品または同一ネット上のゲートウェイ（ルータ）の IP アドレスを入力 ●ネームサーバアドレス 本製品の IP アドレスを入力	●設定方法 ［手入力］を選択（IP アドレス・サブネットマスクを入力） ●ルータアドレス 本製品または同一ネット上のゲートウェイ（ルータ）の IP アドレスを入力 ●ネームサーバアドレス 使用する DNS サーバの IP アドレスを入力

◆DNSの設定について
設定ページの［ルータ設定（LAN）］画面で［LAN側DNSサーバアドレス（プライマリ）］を設定していると、その設定内容がIPアドレスとともに本製品からパソコンに通知されます（DHCPサーバ機能による）。
［LAN側DNSサーバアドレス（プライマリ）］［LAN側DNSサーバアドレス（セカンダリ）］をともに設定していないときは、［DHCPサーバ機能］がOFF、［AutoDNS機能］がONの場合と同様に、各パソコンでDNSサーバのIPアドレスを設定してください。

簡易DNSサーバにする

AutoDNS機能を使うとき、本製品を簡易DNSサーバとして使用できます。簡易DNSサーバは、ドメイン名からIPアドレスを検索するドメイン名解決要求と、IPアドレスからドメイン名を検索するドメイン名逆引き要求に応じます（UDP/53による）。

設定ページ

簡易DNSサーバ機能を使用するには、パソコンのホスト名と対応するIPアドレスの組み合わせを本製品側に登録しておく必要があります。組み合わせは、ホスト情報として最大32個まで登録できます。
頻繁に接続するパソコンは、ホスト情報に登録することをお勧めします。

■［詳細設定］→［ルータ設定］→［LAN］

本製品の IP アドレス／サブネットマスク	192.168.10.1/24
AutoDNS機能	［ON］を選択
オプション	ip host 192.168.10.8 pc-user.mn128soho.co.jp ※この場合、「pc-user.mn128soho.co.jp」または「pc-user」のドメイン名解決要求に応じます。

パソコンの設定

■DHCPサーバ機能がONのとき

パソコン側での設定は不要です。

■DHCPサーバ機能がOFFのとき

パソコン側のDNSサーバの設定で、本製品のIPアドレスを指定する必要があります。

●Windows XPの場合

［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティで、［次のDNSサーバーのアドレスを使う］を選択し、「192.168.10.1」を指定します。

●Windows 2000の場合

［コントロールパネル］→［ネットワークとダイヤルアップ設定］→［ローカルエリア接続］のプロパティで、［次のDNSサーバーのアドレスを使う］を選択し、「192.168.10.1」を指定します。

●Windows 98 SE/Meの場合

［コントロールパネル］→［ネットワーク］→［TCP/IP］のプロパティ→［DNS設定］タブ→［DNSサーバ検索順］に、「192.168.10.1」を指定します。

●Macintoshの場合

［コントロールパネル］→［TCP/IP］→［ネームサーバアドレス］に、「192.168.10.1」を指定します。

◆簡易DNSサーバの動作について

● ドメイン名解決要求を受信したとき

簡易DNSサーバはホスト情報を検索します。一致する情報がある場合、対応するIPアドレスをパソコンに送信します。一致する情報がない場合、通常のAutoDNS機能の動作に従います。

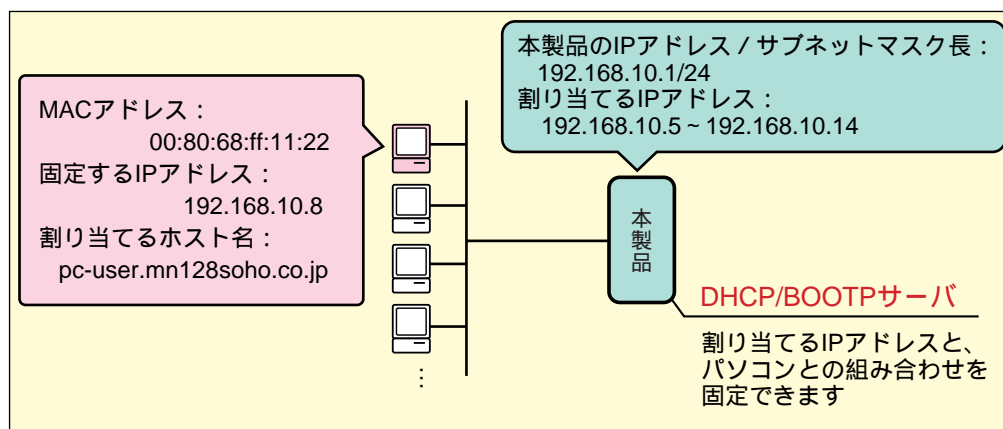
このとき、自動接続の設定をしていると、自動的に接続されるので注意が必要です。また、LAN側だけでなく、WAN側からのドメイン名解決要求にも応じます。

● ドメイン名逆引き要求を受信したとき

簡易DNSサーバはホスト情報を検索します。一致する情報がある場合、最初に登録されているホスト名をパソコンに送信します。

なお、ホスト情報は、DHCP/BOOTPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定する場合にも使われます。「DHCP/BOOTPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定する」〈P.24〉を参照してください。

DHCP/BOOTPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定する

本製品のDHCPサーバ機能を使ってパソコンのIPアドレスを設定する際、パソコンと設定するIPアドレスの組み合わせを固定できます。設定するIPアドレスとパソコンの組み合わせは、ホスト情報として最大32個まで登録できます。

ホスト情報は、本製品を簡易DNSサーバにする場合にも使われます。簡易DNSサーバについては、「簡易DNSサーバにする」〈P.22〉を参照してください。

設定ページ

■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス／サブネットマスク長	192.168.10.1/24
DHCPサーバ機能	［ON］を選択
開始IPアドレス／個数	192.168.10.5/10
オプション	ip host 192.168.10.8 pc-user.mn128soho.co.jp 00:80:68:ff:11:22 ※「192.168.10.8」は必ず「00:80:68:ff:11:22」のパソコンに割り当てられますが、 192.168.10.5〜192.168.10.7 192.168.10.9〜192.168.10.14 は不特定のパソコンに割り当てられます。

DHCP/BOOTPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定する場合は、必ずホスト情報にMACアドレスを登録してください。

◆本製品を簡易DNSサーバにしているとき

本製品を簡易DNSサーバとするために設定したホスト情報（MACアドレスの登録がないホスト情報）を登録した場合も、指定したIPアドレスが［ルータ設定（LAN）］画面の［開始IPアドレス/個数］に該当すると、DHCP/BOOTPサーバ機能が働き、パソコンにIPアドレスが割り当てられます。

例）　ip host 192.168.10.9 pc-user.mn128soho.co.jp

DHCP/BOOTPサーバ機能を使ってIPアドレスを設定する不特定のパソコンに、IPアドレス「192.168.10.9」が割り当てられます。

また、IPアドレス「192.168.10.9」のドメイン名逆引き要求には、「pc-user.mn128soho.co.jp」と応じます。

◆パソコンのMACアドレスを確認する

パソコンのMACアドレスを確認するには、次の方法で行います。

●Windows XPの場合

1. ［スタート］メニュー→［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］の順に選択します。
2. ［ローカルエリア接続］を右クリックし、［状態］を選択します。
   ［ローカルエリア接続の状態］が表示されます。
3. ［サポート］タブをクリックし、［詳細］ボタンをクリックします。
   ［ネットワーク接続の詳細］ダイアログが表示され、［物理アドレス］にMACアドレスが表示されます。

●Windows 2000の場合

1. ［スタート］メニュー→［アクセサリ］→［コマンドプロンプト］の順に選択します。
2. 「ipconfig/all¦more」と入力して［Enter］キーを押します。
3. 「Physical Address」に、MACアドレスが表示されます。

●Windows 98 SE/Meの場合

1. ［スタート］メニュー→［プログラム］→［MS-DOSプロンプト］の順に選択します。
2. 「C:>」の後ろに「winipcfg」と入力します。
   ［IP設定］が開きます。
3. ポップアップメニューから、使用しているEthernetアダプタ名を選択します。
   ［アダプタアドレス］にMACアドレスが表示されます。

●Macintoshの場合

1. アップルメニュー→［Appleシステム・プロフィール］を選択します。
2. ［システム特性］タブ→［ネットワーク概略］→［AppleTalk］の［ハードウェアアドレス］に、MACアドレスが表示されます。

パソコン3台のうち特定の1台だけで インターネットに接続する（端末型）

LAN上のパソコンのうち、特定のIPアドレスのパソコンだけでインターネットに接続するには、「IPアドレス変換（NAT）テーブル」を設定する必要があります。なお、それ以外のパソコンはインターネットに接続できません。

設定ページ

■ ［詳細設定］ → ［接続／相手先登録］ → ［#1］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
通信チャネル	［PPPoE（ランプ点灯）］を選択
接続モード	［端末型接続］を選択

■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス／サブネットマスク長	192.168.0.1/24
DHCPサーバ機能	OFF
オプション	ip nat 1 192.168.0.1-192.168.0.2/*/* ipcp ※ 192.168.0.1 が含まれないと、AutoDNS 機能やメール着信通知機能が使用できません。 ※「ipcp」を設定すると、プライベート IP アドレスと、PPPoE（端末型）での接続または端末型ダイヤルアップ接続時に割り当てられる IP アドレスの変換になります。

意図しない接続が起こらないように、［料金による制限］［接続回数による制限］［最大接続時間］［時間帯による制限］を設定することをお勧めします。

パソコンの設定

■パソコンのTCP/IPの設定を変更して、固定のIPアドレスを割り当てます。

1. LAN上のパソコンにすべて、プライベートIPアドレスを割り当てます。次のダイアログで設定します。

   Windows XP ：［コントロールパネル］→［ネットワークとインターネット接続］→［ネットワーク接続］→［ローカルエリア接続］のプロパティ］
   Windows 2000 ：［コントロールパネル］→［ネットワークとダイヤルアップ接続］→［ローカルエリア接続］のプロパティ
   Windows 98 SE/Me ：［コントロールパネル］→［ネットワーク］
   Macintosh ：［コントロールパネル］→［TCP/IP］

2. パソコンを再起動します。

パソコン10台のうち特定の5台だけで インターネットに接続する（端末型）

LAN上のパソコンのうち、特定のIPアドレスのパソコンだけインターネットに接続させるには、「IPアドレス変換（NAT）テーブル」を設定します。さらに、DHCP/BOOTPサーバ機能で、本製品から特定のパソコンに、常に特定のIPアドレスアドレスを割り当てます。

設定ページ

■［詳細設定］→［接続／相手先登録］→［#1］

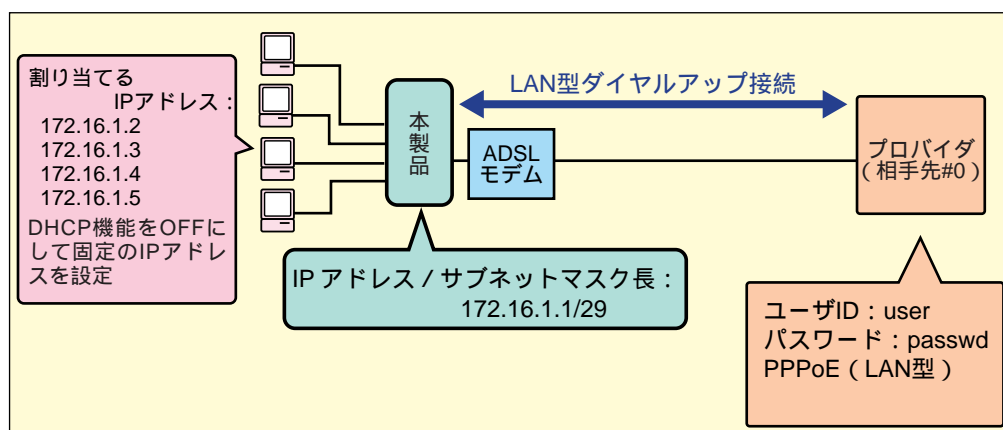
相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
通信チャネル	［PPPoE（ランプ点灯）］を選択
接続モード	［端末型接続］を選択

■［詳細設定］→［ルータ設定］→［LAN］

項目	設定値
本体の IP アドレス／サブネットマスク長	192.168.0.1/24
DHCP サーバ機能	ON
開始 IP アドレス／個	192.168.0.2/10
オプション	ip nat 1 192.168.0.1-192.168.0.6 ipcp ip host 192.168.0.2 user1.tmp.co.jp 0a:1b:2c:00:11:22 ip host 192.168.0.3 user2.tmp.co.jp 0a:1b:2c:00:11:23 ip host 192.168.0.4 user3.tmp.co.jp 0a:1b:2c:00:11:24 ip host 192.168.0.5 user4.tmp.co.jp 0a:1b:2c:00:11:25 ip host 192.168.0.6 user5.tmp.co.jp 0a:1b:2c:00:11:26 （user5.tmp.co.jp：任意のホスト名を割り当てます。　0a:1b:2c:00:11:26：パソコンのMACアドレスです。） ※同じパソコンに同じIPアドレスが割り当てられるようにします。

意図しない接続が起こらないように、［料金による制限］［接続回数による制限］［最大接続時間］［時間帯による制限］を設定することをお勧めします。

PPPoE（IPアドレス払い出し）LAN型ダイヤルアップ接続する

本製品のLANポートに接続したパソコン（またはハブを経由したパソコン）から、プロバイダにLAN型ダイヤルアップ接続する場合の設定例を紹介します。

プロバイダとLAN型ダイヤルアップ接続の契約をする必要があります。

設定ページ

■［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
通信チャネル	PPPoE（ランプ点灯）
接続モード	［LAN 型接続］を選択

■［詳細設定］→［ルータ設定］→［LAN］

本体の IP アドレス / サブネットマスク	172.16.1.1/29
DHCP サーバ機能	OFF

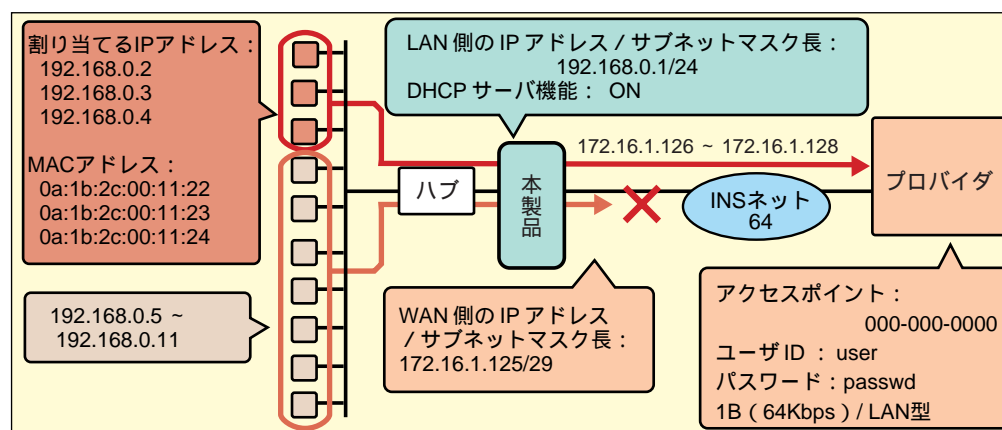
操作

■手動接続します

1. ［詳細設定］→［接続／相手先登録］で、接続したい相手先番号（例では#0）をクリックします。

2. ［以下の相手先に回線を接続する。］をクリックし、［実行］ボタンをクリックします。

パソコン10台のうち特定の3台だけで インターネットに接続する（LAN型）

LAN型ダイヤルアップで相手先と接続しているとき、特定のパソコンだけをインターネットに接続させるために、「IPアドレス変換（NAT）」テーブルを設定します。

設定ページ

■ [詳細設定] → [接続／相手先登録] → [#0]

相手先名称	名称（何でも構いません）を設定
相手先電話番号	000-000-0000
送信ユーザ ID	user
送信パスワード	passwd
通信チャネル	1B（64Kbps）
接続モード	[LAN 型接続] を選択

■［詳細設定］→［ルータ設定］→［LAN］

本体の IP アドレス／サブネットマスク長	192.168.0.1/24
DHCP サーバ機能	ON
開始 IP アドレス／個	192.168.0.2/10
オプション	ip nat 1 192.168.0.1/*/* 172.16.1.125 ip nat 2 192.168.0.2/*/* 172.16.1.126 ip nat 3 192.168.0.3/*/* 172.16.1.127 ip nat 4 192.168.0.4/*/* 172.16.1.128 ip host 192.168.0.2 user1.tmp.co.jp 0a:1b:2c:00:11:22 ip host 192.168.0.3 user2.tmp.co.jp 0a:1b:2c:00:11:23 ip host 192.168.0.4 user3.tmp.co.jp 0a:1b:2c:00:11:24 （user3.tmp.co.jp：任意のホスト名を割り当てます。）（0a:1b:2c:00:11:24：パソコンのMACアドレスです。） ※同じパソコンに同じIPアドレスが割り当てられるようにします。

専用線でインターネットに接続する

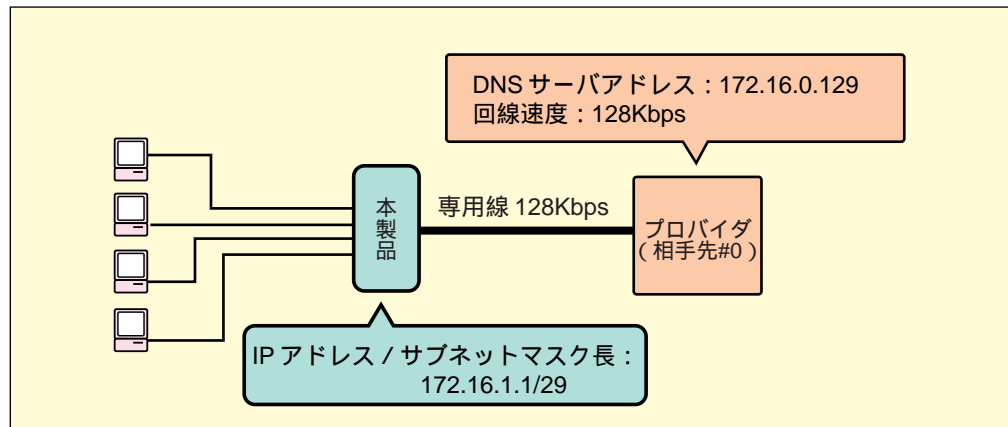
確認

ハイ・スーパーディジタル回線（専用線）への加入契約はお済みですか？契約されていない場合は、注意事項をお読みの上、手続きを行ってください。詳しくは、最寄りのNTTまでお問い合わせください。

◎ハイ・スーパーディジタル回線を使用するとき

「NTT専用契約申込書」の次の項目に、必要な内容を記載してください。

- 「③ 契約形態」
  「単独専用」を選択してください。
- 「④ 品名」
  通信スピードを64Kbpsにするときは「HSD 64Kbps/s(I)」と記入してください。
  通信スピードを128Kbpsにするときは「HSD 128Kbps/s(I)」と記入してください。
- 「⑤ 回線数」
  4線式：1
- 「⑦ 端末設備の品名等」
  品名：MN128-SOHO IB3
  製造会社名：（株）NTT-ME
  適合認定番号：本体背面のシールを参照して、記入してください。
- 「⑧ 端末設備の設置場所」
  （1）起点/（2）終点の設置場所：本製品を設置する場所の住所と電話番号を記入してください。
  品目番号及び台数：「⑦ 端末設備の品名等」で「MN128-SOHO IB3」と記入した欄の番号と、台数を記入してください。
  　例）（1）×1
  引き込み・配線工事区分：NTTがすべて施工する場合は「端末直前まで」を選択してください。
- 「⑩ 分岐」
  分岐：無
- 「⑪ 使用態様」
  他回線との接続：無

ここでは、専用線を利用してインターネットにアクセスする例を解説します。

専用線で接続する場合、必ず接続/相手先登録の「#0」が使用されます。

設定ページ

■ [詳細設定] → [接続／相手先登録] → [#0]

相手先名称	名称（何でも構いません）を設定
DNS サーバアドレス	172.16.0.129

■ [詳細設定] → [ルータ設定] → [ISDN]

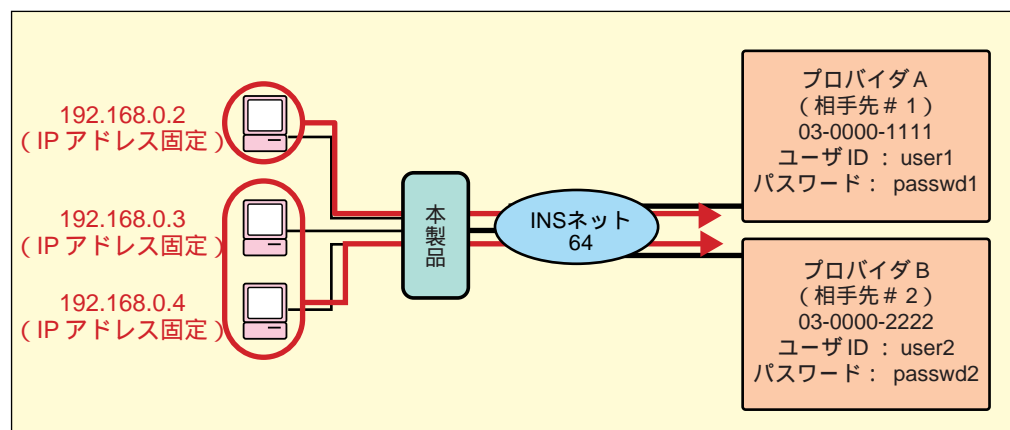
回線種別	専用線 128Kbps

■ [詳細設定] → [ルータ設定] → [LAN]

本体のIPアドレス／サブネットマスク長	172.16.1.1/29

3 複数のプロバイダに接続する

本製品に接続したパソコン3台のうち 1台はプロバイダAへほかの2台はプロバイダBへ

「ソースルーティング機能」を使用して、本製品に接続した3台のパソコンで、別々のプロバイダに接続できます。

設定ページ

■ [詳細設定] → [接続／相手先登録] → [#1]

相手先名称	プロバイダAの名称（何でも構いません）を設定
相手先電話番号	03-0000-1111
送信ユーザID	user1
送信パスワード	passwd1
接続モード	[端末型接続] を選択

■ [詳細設定] → [接続／相手先登録] → [#2]

相手先名称	プロバイダBの名称（何でも構いません）を設定
相手先電話番号	03-0000-2222
送信ユーザID	user2
送信パスワード	passwd2
接続モード	[端末型接続] を選択

■ ［詳細設定］ → ［自動接続相手先］

自動接続相手先 1	なし
自動接続相手先 2	なし

■ ［詳細設定］ → ［ルータ設定］ → ［LAN］

本体のIPアドレス／ サブネットマスク長	192.168.0.1/24
DHCP サーバ機能	OFF
オプション	ip srcroute 192.168.0.2/32 remote 1 static ip srcroute 192.168.0.3/32 remote 2 static ip srcroute 192.168.0.4/32 remote 2 static

操作

■手動接続します

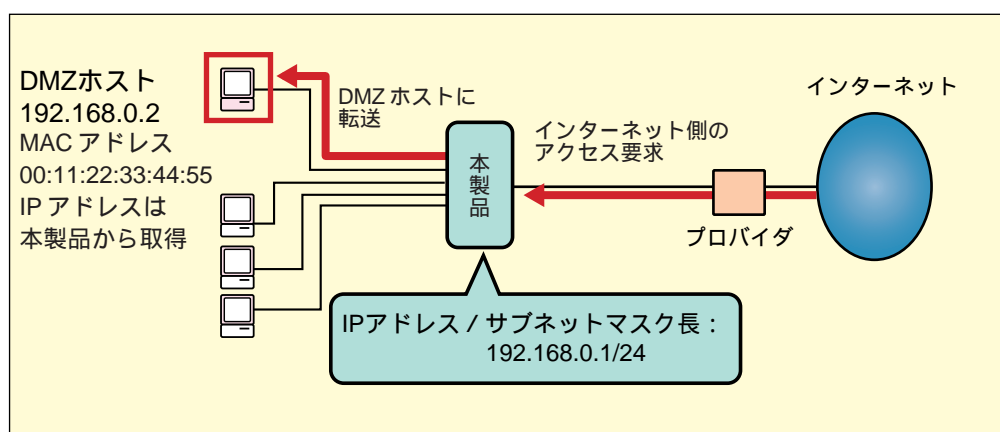
1. ［詳細設定］ → ［接続／相手先登録］ で、接続したい相手先番号（#1または#2）をクリックします。

2. ［以下の相手先に回線を接続する。］ をクリックし、［実行］ ボタンをクリックします。

192.168.0.2のパソコンを利用するときは相手先＃1を接続、192.168.0.3、192.168.0.4のパソコンを利用するときは相手先＃2を接続してください。違う相手先に接続しても通信はできませんが、回線は接続されるため、料金が発生してしまいます。

AutoDNS機能を使用する場合、DNS要求は最初に接続したプロバイダのDNSサーバから順に転送されます。

DMZホストを設定する

DMZホスト機能を設定すると、IPアドレス（変換）テーブルで変換できない、インターネット側から発信された宛先不明のパケットを、特定のパソコンに転送できます。使用ポートが特定できないネットワークゲームなどのアプリケーションを利用するときや、外部にサーバを公開するときなどに設定すると便利です。

◆DMZホスト機能は、端末型でインターネットに接続しているときのみ有効です。
◆DMZホストになったパソコンは、インターネット側からの攻撃を受けやすくなるので注意してください。

設定ページ

■［詳細設定］→［セキュリティ］

DMZホストアドレス	192.168.0.2

■［詳細設定］→［ルータ設定］→［LAN］

オプション	ip host 192.168.0.2 dhost.mn128soho.co.jp 00:11:22:33:44:55 （dhost.mn128soho.co.jp：任意のホスト名を割り当てます。） （00:11:22:33:44:55：パソコンのMACアドレスです。）

DMZホストを登録した場合、クイック設定をしたときに自動的に追加されるフィルタによって、外部からTCPによる通信ができない場合があります。その場合は、tcpestを禁止するフィルタを削除するか、またはtcpを通過させるフィルタを追加してください。

※クイック設定で自動的に追加されるフィルタについては、「クイック設定で自動的に設定されるフィルタ」〈P.137〉を参照してください。

・tcpを追加させるフィルタの設定例

接続相手先 → #0

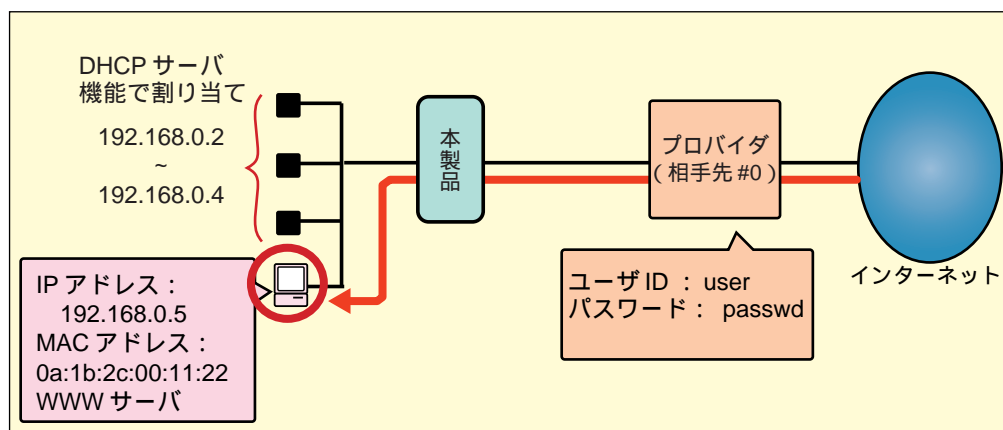
DMZホストのIPアドレス → 192.168.0.2

```
ip filter 10 pass in * 192.168.0.2/32 tcpest * * remote 0
ip filter 11 pass in * 192.168.0.2/32 tcp * * remote 0
```

※フィルタ番号の「10」「11」は一例です。設定環境に合わせて番号を書き換えてください。

上記2つのフィルタを追加します。

WWWサーバを公開する（端末型）

プロバイダにPPPoE端末型で接続したときに、こちら側のWWWサーバを公開する例を紹介します。

通常、プロバイダにPPPoE端末型で接続したときは、相手先からはこちらのサーバを利用することはできません。
本製品では、相手先に対して、WWWサーバの利用に必要なサービス（WWW、ftpなど）を使用できるように設定できます。相手先に各種サービスの利用を許可するには、IPアドレス変換（NAT）テーブルおよびIPフィルタを使います。IPアドレス変換（NAT）テーブルは32個、IPフィルタは64個まで設定できます。

◆インターネットにサーバを公開すると、外部からの攻撃などの被害に遭う可能性があります。セキュリティ対策を十分に行ってください。

◆本製品にはステートフル・パケット・インスペクション（SPI）機能〈P.78〉が工場出荷時の状態でONになっています。この機能をOFFにすると、IPフィルタを使用しないで各種サービスの利用を許可することができますが、セキュリティのレベルが下がるので注意してください。

設定ページ

■［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
通信チャネル	［PPPoE（ランプ点灯）］を選択
接続モード	［端末型接続］を選択

■［詳細設定］→［ルータ設定］→［LAN］

オプション	ip filter 1 pass in * 192.168.0.5 tcp * www remote 0 ip nat 1 192.168.0.5/tcp/www ipcp remote 0 ip nat 2 */*/* ipcp remote 0 ip host 192.168.0.5 host.mn128soho.co.jp 0a:1b:2c:00:11:22 （host.mn128soho.co.jp：任意のホスト名を割り当てます。） （0a:1b:2c:00:11:22：パソコンのMACアドレスです。）

相手先は、本製品がIPCPで取得したIPアドレスを使って、こちら（本製品）側のWWWサーバにアクセスできます。なお、IPCPで取得したIPアドレスは、［切断／接続情報］→［PPPoE］画面の［割当IPアドレス］で確認できます。

このほか、セキュリティのためインターネット側からの不正パケット破棄したり、意図しない接続を禁止するIPフィルタの設定をすることをお勧めします。フィルタの設定については、「IPフィルタの設定」〈P.83〉をお読みください。

◆ PPPoE端末型（端末型ダイヤルアップ）接続時のIPアドレス変換（NAT）テーブルの登録

IPアドレス変換（NAT）を登録しなくても、本製品からPPPoE端末型（または端末型ダイヤルアップ）でインターネットに接続すると、LAN上のすべてのパソコンから相手先にアクセスすることができます。これは、AutoNAT機能によって、すべてのプライベートIPアドレスが自動的に取得するグローバルIPアドレスに変換されるためです。IPアドレス変換（NAT）テーブルは必要に応じて登録してください。

◆ ポート番号の変換について

NATのコマンドにポート番号設定用のパラメータを指定すると、ポート番号を変換できます。

・書式

ip nat {nnumber private[-range][/protocol/p_port[-range]] global[/g_port] [interface] [rnumber] [latest]}

・パラメータ

nnumber	：	NATテーブル番号 [1～32]
private	：	プライベートアドレス（「start-end」で範囲指定、「＊」は全て）
protocol	：	「esp」，「gre」，「icmp」，「ipencap」，「tcp」，「udp」（「＊」は全て）
p_port	：	プライベートポート番号、またはニーモニック（「start-end」で範囲指定、「＊」は全て） ニーモニック：「ftp」，「ftpdata」，「telnet」，「smtp」，「www」，「pop3」，「sunrpc」，「nntp」，「ntp」，「login」，「pptp」，「domain」，「route」，「who」
global	：	グローバルアドレス（「ipcp」はIPCP、「dhcp」はDHCP、「dynamic」はIPCPまたはDHCPで取得するアドレス）
g_port	：	グローバルポート番号、またはニーモニック（「＊」は指定無し） ニーモニック：「ftp」，「ftpdata」，「telnet」，「smtp」，「www」，「pop3」，「sunrpc」，「nntp」，「ntp」，「login」，

「pptp」,「domain」, 「route」,「who」

interface　：「remote」または「wanether」(省略時または「＊」は全て)

rnumber　：相手先番号 [0～15]

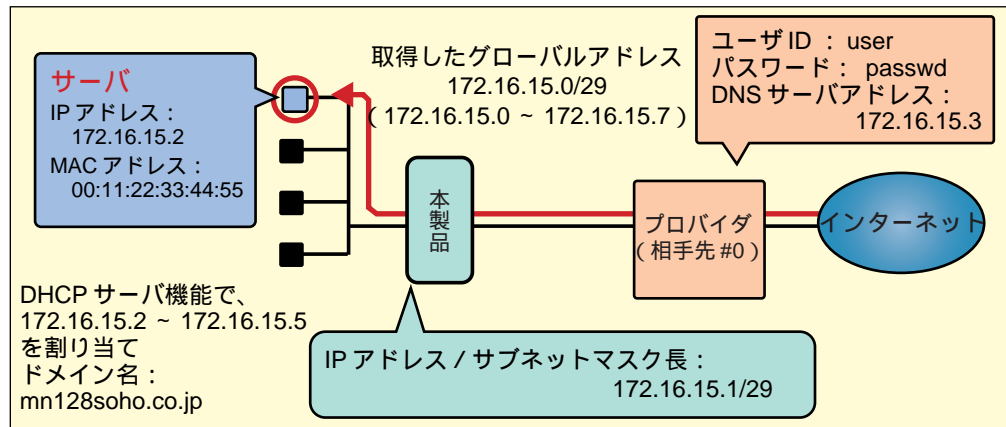
latest　：「latest」

※グローバルポート番号を指定した場合は、プライベートIPアドレス、プロトコル、プライベートポート番号を一意に設定する必要があります。プロトコルをTCPまたはUDP以外に設定したり、IPアドレスの指定を省略または範囲指定にすることはできません。

◆ PPPoE端末型（端末型ダイヤルアップ）接続時や本製品に登録したNATテーブルを使った通信時のRIPについて

PPPoE端末型（端末型ダイヤルアップ）接続時や、WANポートに固定IPアドレスを設定したとき、DHCPサーバからIPアドレスを取得したときは、本製品に登録したNATテーブルを使った通信時、本製品は相手先にRIPを送信しません。

サーバを立ち上げて外部に公開する（NAT未使用）

ここでは、グローバルIPアドレスを複数取得してLANを運用し、WWW、FTP、DNS、メールサーバを公開する例をご紹介します。

※上記の場合、172.16.15.0、172.16.15.7は端末には割り当てられません。

インターネットにサーバを公開すると、外部からの攻撃などの被害に遭う可能性があります。セキュリティ対策を十分に行ってください。

設定ページ

■［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
DNS サーバアドレス	172.16.15.3
通信チャネル	PPPoE（ランプ点灯）
接続モード	［LAN 型接続］を選択

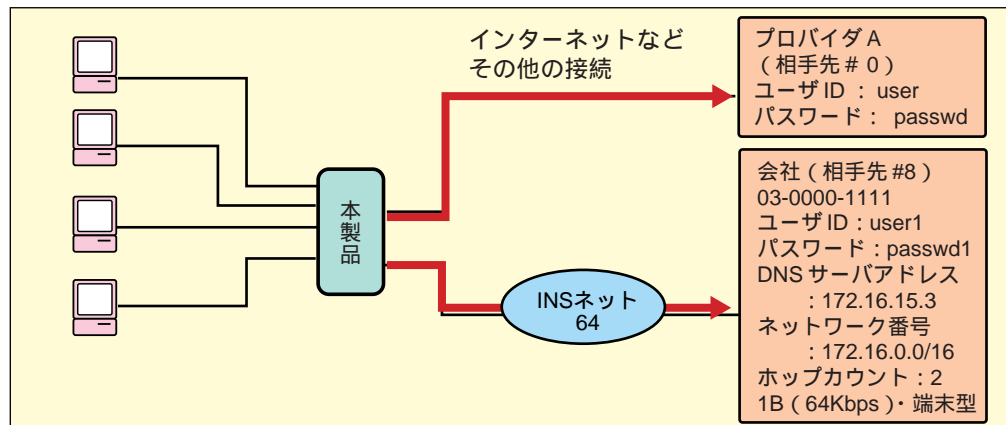
■ [詳細設定] → [ルータ設定] → [LAN]

項目	設定
本体の IP アドレス / サブネットマスク長	172.16.15.1/29
DHCP サーバ機能	ON
開始 IP アドレス / 個数	172.16.15.2/4
ドメイン名	mn128soho.co.jp
オプション	●次のコマンドを設定 ip filter 20 pass in * 172.16.15.2 tcp * pop3 remote 0 ip filter 21 pass in * 172.16.15.2 tcp * www remote 0 ip filter 22 pass in * 172.16.15.2 tcp * 443 remote 0 ip filter 23 pass in * 172.16.15.2 tcp * smtp remote 0 ip filter 24 pass in * 172.16.15.2 tcp * domain remote 0 ip filter 25 pass in * 172.16.15.2 udp * domain remote 0 ip filter 26 pass in * 172.16.15.2 tcp * 113 remote 0 ip filter 27 pass in * 172.16.15.2 tcp * ftp remote 0 ip filter 28 pass in * 172.16.15.2 tcp * ftpdata remote 0 ip filter 29 pass in * 172.16.15.2 tcp * 1024-65535 remote 0 ip filter 30 pass in * 172.16.15.2 udp * 1024-65535 remote 0 ip filter 31 reject in * 172.16.15.2 udp * * remote 0 ip host 172.16.15.2 host.mn128soho.co.jp 00:11:22:33:44:55 （host.mn128soho.co.jp：任意のホスト名を割り当てます。 00:11:22:33:44:55：パソコンのMACアドレスです。）

※IP filter21、22はWWWサーバへのアクセスを通すためのフィルタです。
※IP filter20、23、26はメールサーバへのアクセスを通すためのフィルタです。
※IP filter24、25はDNSへのアクセスを通すためのフィルタです。
※IP filter27、28はftpdataとftpパケットを通すためのフィルタです。
※IP filter29、30は外部からの送信ポートが1024番以降（WellKnownポート以外）を通すためのフィルタです。
※IP filter31は上記以外のアクセスを破棄するためのフィルタです。

このほか、セキュリティのためインターネット側からの不正パケット破棄したり、意図しない接続を禁止するIPフィルタの設定をすることをお勧めします。フィルタの設定については、「IPフィルタの設定」〈P.83〉をお読みください。

ブロードバンド接続しながら ISDN回線で会社に接続する

ここでは、プロバイダにPPPoE端末型で接続してインターネットにアクセスし、同時にISDN回線を利用して会社に接続するための設定例を解説します。

※ホップカウントは、本製品から会社までの経路にあるルータの数です。本製品は含みません。

設定ページ

■プロバイダに接続するための設定

●［クイック設定］→［PPPoE（端末型)］→PPPoE設定：メイン

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd

■ISDN回線を利用して会社に接続するための設定

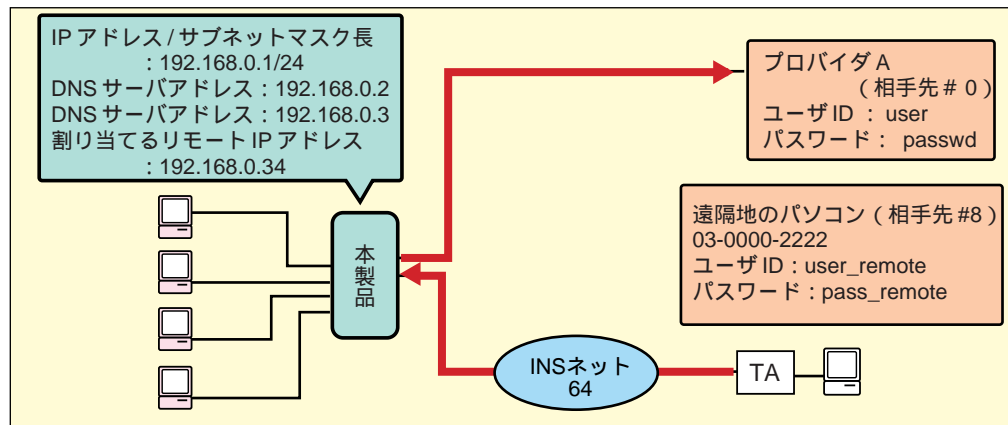
● [詳細設定] → [接続/相手先登録] → [#8]

相手先名称	名称（何でも構いません）を設定
相手先電話番号	03-0000-1111
送信ユーザ ID	user1
送信パスワード	passwd1
DNS サーバアドレス	172.16.15.3
通信チャネル	1B（64kbps）を選択
接続モード	[端末型接続] を選択

● [詳細設定] → [ルータ設定] → [LAN]

オプション	ip route 172.16.0.0/16/2 remote 2 static ※上記は、会社に接続するための IP アドレス経路情報です。「172.16.0.0/16」は会社のネットワーク番号です。「static」を指定すると、手動での接続になります。 ※会社に自動接続するときは、次のように入力します。 ip route 172.16.0.0 /16/2 remote 2 auto ISDN 回線を利用して自動接続する場合は、IP アドレス経路情報を登録します。[自動接続相手先] 画面で、相手先を指定しないでください。

ブロードバンド接続しながら ISDN回線で遠隔地のパソコンから着信を受ける

ここでは、プロバイダにPPPoE端末型で接続してインターネットにアクセスし、同時にISDN回線を利用して遠隔地のパソコンからリモートアクセスするための設定例を解説します。

設定ページ

■プロバイダに接続するための設定

● ［クイック設定］ → ［PPPoE（端末型)］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd

■遠隔地のパソコンから本製品にリモートアクセスするための設定

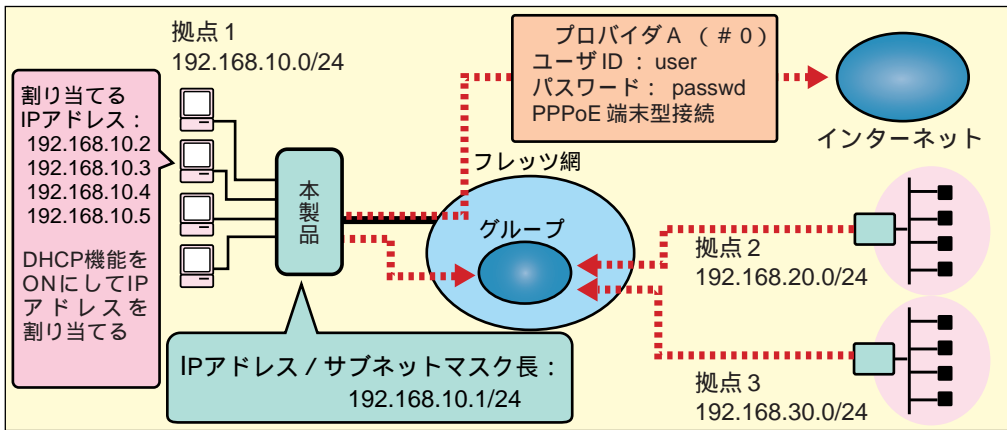
●［詳細設定］→［接続／相手先登録］→［#8］

相手先名称	名称（何でも構いません）を設定
相手先電話番号	03-0000-2222
相手からの着信	［応じる］
受信ユーザ ID	user_remote
受信パスワード	pass_remote

●［詳細設定］→［ルータ設定］→［LAN］

本体の IP アドレス / サブネットマスク長	192.168.0.1/24
AutoDNS 機能	ON
LAN 側 DNS サーバアドレス（プライマリ） /LAN 側 DNS サーバアドレス（セカンダリ）	192.168.0.2 192.168.0.3
リモートアクセスサーバ機能	ON
リモート IP アドレス	192.168.0.34

フレッツ・グループアクセスを利用する

フレッツ・グループアクセスは、フレッツ・ADSL、Bフレッツ、フレッツISDNを利用して、プライベートネットワークを構築し、グループに登録されているメンバー間での通信を可能にするサービスです。
ここでは、フレッツ・グループアクセス・プロを契約して、メインセッションはプロバイダへ接続、サブセッションでフレッツ・グループアクセスへPPPoEで接続する例を解説します。

設定ページ

■プロバイダに接続するための設定

● ［クイック設定］ → ［PPPoE（端末型）：メイン］

ログインユーザ ID	設定ページを開くためのユーザ ID を入力します。
ログインパスワード	設定ページを開くためのパスワードを入力します。
ログインパスワード（再入力）	上記で設定したパスワードをもう一度入力します。
接続設定：メイン 以下の内容で設定を行う	チェックする
相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd

ログインユーザIDとログインパスワードは、インターネット側から本製品の設定ページへ不正にアクセスできないようにするために設定します。
［接続設定：メイン］で、契約しているプロバイダの設定を行います。

■フレッツ・グループアクセスの設定

● ［詳細設定］ → ［接続／相手先設定］ → ［＃7］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	フレッツ・グループアクセス・プロで割り当てられたユーザ ID を入力
送信パスワード	フレッツ・グループアクセス・プロで割り当てられたパスワードを入力
通信チャネル	PPPoE（ランプ点灯）を選択
接続モード	［LAN 型接続］を選択

● ［詳細設定］ → ［本体設定］ → ［LAN］

本体のIPアドレス／サブネットマスク長	192.168.10.1/24 ※フレッツ・グループアクセス・プロで割り当てられたIPアドレスを設定します。
DHCPサーバ機能	ONを選択
開始IPアドレス/個数	192.168.10.2/4 ※フレッツ・グループアクセス・プロで割り当てられたIPアドレスを設定します。 ※割り当てるIPアドレスのうち、最初のIPアドレスと、割り当てるIPアドレスの個数を入力します。
オプション	ip filter 1 pass out 192.168.10.1-192.168.10.5 * * * * remote 7 ip filter 2 pass in 192.168.20.0/24 * * * * remote 7 ip filter 3 pass in 192.168.30.0/24 * * * * remote 7 ip filter 4 reject out * * * * * remote 7 ip filter 5 reject in * * * * * remote 7 ip route 192.168.20.0/24/2 remote 7 static ip route 192.168.30.0/24/2 remote 7 static

フレッツ・ISDNのときインターネットへの接続とフレッツ・スクウェアへの接続を使い分ける

ここでは、フレッツ・ISDNを契約して、プロバイダへの接続をメインに、フレッツ・スクウェアの接続をサブに設定して、必要に応じて使い分ける方法を解説します。

設定ページでは、複数の接続相手先を登録できますが、フレッツ・ISDNで同時に接続できる相手先は1つです。

設定ページ

■［クイック設定］→［フレッツ・ISDN：メイン］

ログインユーザ ID	設定ページを開くためのユーザ ID を入力します。
ログインパスワード	設定ページを開くためのパスワードを入力します。
ログインパスワード（再入力）	上記で設定したパスワードをもう一度入力します。
接続設定：メイン 以下の内容で設定を行う	チェックする
相手先名称	名称（何でも構いません）を設定
相手先電話番号	000-000-0000
送信ユーザ ID	user
送信パスワード	passwd

ログインユーザIDとログインパスワードは、インターネット側から本製品の設定ページへ不正にアクセスできないようにするために設定します。
［接続設定：メイン］で、契約しているプロバイダの設定を行います。

■［クイック設定設定］→［フレッツ・ISDN：サブ＃1］

接続設定：サブ　#1 以下の内容で設定を行う	チェックする
相手先名称	フレッツ・スクウェア（NTT 東日本）
相手先電話番号	1492
送信ユーザ ID	guest@flets
送信パスワード	guest
宛先ドメイン名 / 宛先アドレス	.flets ※このドメインルーティングを使用するときは、AutoDNS 機能を ON にしてください（工場出荷時の設定は ON です）。

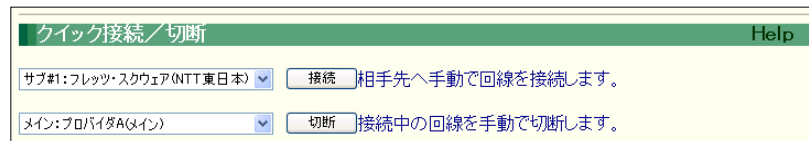
本製品では、［サブ#1］でフレッツ・スクウェア（NTT東日本）の、［サブ#2］でフレッツ・スクウェア（NTT西日本）の設定が用意されています。お住まいのエリアによって、どちらかの設定をチェックしてください。

操作

■フレッツ・スクウェアに接続するとき

フレッツ・ISDNをご利用の場合は、同時に複数の相手先に接続することはできません。フレッツ・スクウェアをご利用になるときは、いったんプロバイダへの接続を切断する必要があります。

1. ［クイック設定］→［フレッツ・ISDN］をクリックします。
   ［ISDNクイック設定（フレッツ・ISDN）］画面が表示されます。

2. 画面をスクロールさせ、［クイック接続／切断］の項目を表示します。
   接続状況が表示されています。

3. メインの回線を切断します。［メイン（相手先名称）］を選択してから［切断］ボタンをクリックします。

   「回線を切断しました。」と表示されます。［OK］ボタンをクリックすると、もとの画面に戻ります。

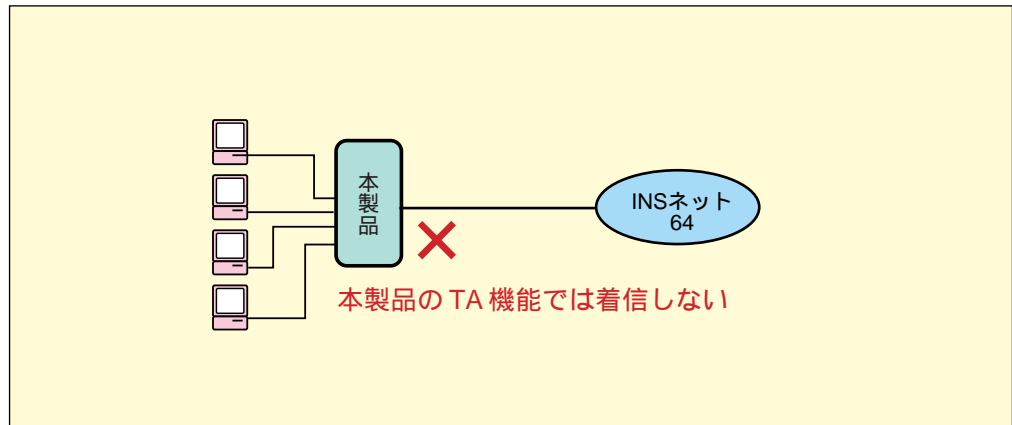
4. フレッツ・スクウェアに接続します。［サブ#1（NTT東日本）］を選択してから［接続］ボタンをクリックします。

   ※NTT西日本のフレッツ・スクウェアをご利用の場合は、［サブ#2（NTT西日本）］を選択してください。

   「接続しました。」と表示されます。［OK］ボタンをクリックすると、もとの画面に戻ります。

   インターネットへ接続したいときは、同じ要領で［サブ#1］の回線を切断し、［メイン］の回線をつなぎます。
   なお、回線の接続・切断状況は、［切断／接続状況］→［ISDN］画面で確認できます。

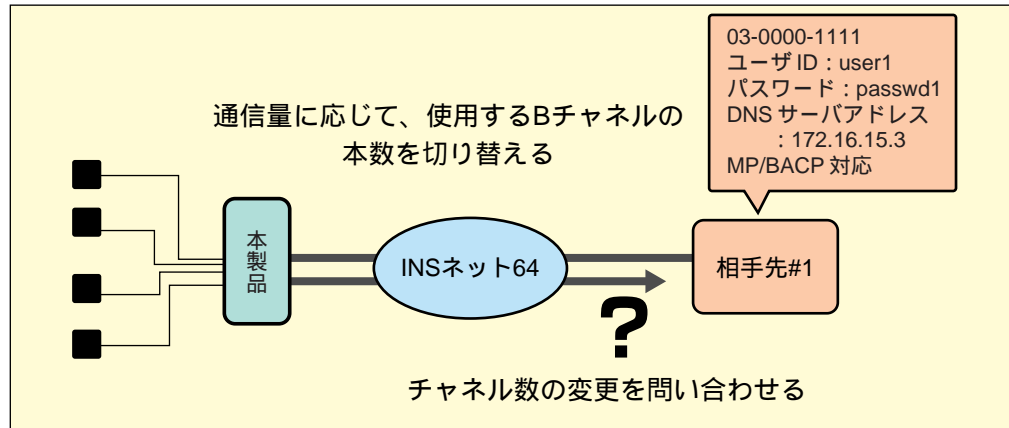
本製品のTA機能で着信しない ISDN

本製品のTA機能ではデータを着信しない場合、データ通信は本製品のルータ機能のみの場合、または本製品のRS-232Cシリアルポートに機器を接続していない場合に、本製品のTA機能をOFFにします。

設定ページ

■ ［詳細設定］ → ［TA］

TA への着信	しない

スループットBOD機能/BACP機能を使う

スループットBOD機能とBACP機能を使うと、通信量に応じて使用するBチャネルの本数を切り替えることができます。

スループットBOD機能は、接続先の要求やこちら側の必要に応じて、使用するチャネル数を自動的に変更する機能です。この機能を使用すると、データ通信量の多いときには2Bチャネルで通信し、少ないときは1Bチャネルで通信できるため、効率良く通信できます。しかし、スループットBODの設定によっては、チャネルの増減が頻繁に発生して、逆に無駄が発生して通信料金がかさむことがあります。
BACPを利用した通信では、使用するチャネル数を変更する前に相手先に問い合わせ、また相手先からチャネル数の変更要求があればそれに応答します。一方的にチャネル数を変更するのではなく、そのつど通信状態を確認しながらチャネル数の増減を行うので、無駄な接続・切断をさけることができます。

スループットBOD機能やBACP機能を使うことができるのは、相手先が次のプロトコルに対応している場合に限ります。
・スループットBOD　：相手先がMPに対応している
・BACP機能　　　　：相手先がMPとBACPに対応している

設定ページ

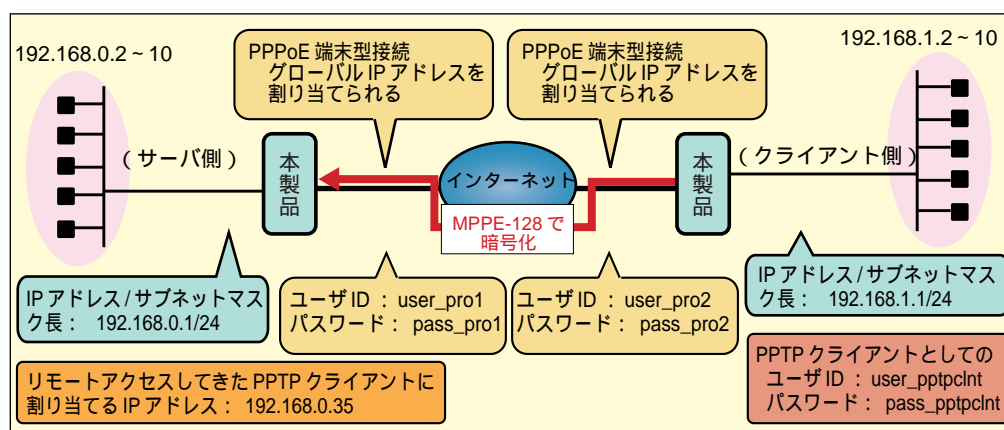
■［詳細設定］→［接続／相手先登録］→［#1］

相手先名称	名称（何でも構いません）を設定
相手先電話番号	03-0000-1111
送信ユーザ ID	user
送信パスワード	passwd
DNS サーバアドレス	172.16.15.3
通信チャネル	可変（BOD+BACP）を選択
接続モード	［端末型接続］を選択

◆ 通信チャネルの選択方法
チャネル数の変更をどのように行うか、その内容によって次の通信チャネルを選択してください。

通信チャネル	チャネル数の変更方法
1B（64Kbps/MP+BACP）	はじめに1Bで接続、1B/2Bの切り替えを手動で行う
2B（128Kbps/MP+BACP）	はじめに2Bで接続、1B/2Bの切り替えを手動で行う
可変（BOD+BACP）	データ量に応じて1B/2Bを自動的に切り替える

PPTPを利用して本製品同士でVPNを構築する

本製品は、PPTPサーバ・PPTPクライアント機能を搭載しているので、PPTPによるVPNを構築できます。ここでは、PPPoE端末型でプロバイダに接続し、本製品同士でVPNを構築する例を解説します。

VPN（Virtual Private Network、仮想プライベートネットワーク）とは、トンネリングやデータの暗号化などのセキュリティ技術を使って、インターネットを仮想的に専用線で接続したWANのように利用するための技術です。PPTP（Point to Point Tunneling Protocol）は、VPNを構築するための代表的なプロトコルです。

PPTPを利用したVPNを構築するときは、本製品にグローバルIPアドレスが割り当てられている必要があります。プライベートIPアドレスを使用している一部のプロバイダでは、VPNを構築できない場合があります。あらかじめご了承ください。

同じネットワークアドレスを設定しているLANを接続することはできません。どちらかのLAN側のサブネットワークアドレスを変更してください。

設定ページ

■サーバ側で設定する内容

●PPPoE端末型でプロバイダに接続するための設定

- ［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user_pro1（プロバイダから通知されたユーザ ID）
送信パスワード	pass_pro1（プロバイダから通知されたパスワード）
通信チャネル	PPPoE（ランプ点灯）
接続モード	端末型接続

●PPTPサーバとしての設定

- ［詳細設定］→［接続／相手先登録］→［#8］

相手先電話番号	空欄にする（クライアントを特定しません。） ※ PPPoE 端末型接続時に、クライアント側に割り当てられたグローバル IP アドレスを入力することもできます。 ※割り当てられたグローバル IP アドレスは、クライアント側の［切断／接続状況］→［PPTP］画面の［割当 IP アドレス］で確認できます。
相手からの着信	［応じる］を選択
受信ユーザ ID	user_pptpclnt （PPTPクライアントが発信してくるユーザID）
受信パスワード	pass_pptpclnt （PPTP クライアントが発信してくるパスワード）
認証プロトコル	MS-CHAPv2
暗号化	MPPE-128

- ［詳細設定］→［ルータ設定］→［LAN］

リモートアクセスサーバ	［ON］を選択
リモート IP アドレス 1	192.168.0.35
オプション	ip filter 2 pass in * 192.168.0.1 tcp * pptp remote 0 ip filter 3 pass in * 192.168.0.1 gre * * remote 0 ip nat 2 192.168.0.1/tcp/pptp ipcp remote 0 ip nat 3 192.168.0.1/gre ipcp remote 0 ip nat 4 */*/* ipcp remote 0

■クライアント側で設定する内容

●PPPoE端末型でプロバイダに接続するための設定

・［詳細設定］→［接続／相手先登録］→［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user_pro2（プロバイダから通知されたユーザ ID）
送信パスワード	pass_pro2（プロバイダから通知されたパスワード）
通信チャネル	PPPoE（ランプ点灯）
接続モード	端末型接続

●PPTPクライアントとしての設定

・［詳細設定］→［接続／相手先登録］→［#8］

相手先電話番号	サーバ側が PPPoE 端末型接続時に、プロバイダから割り当てられたグローバル IP アドレスを入力します。 ※割り当てられたグローバル IP アドレスは、サーバ側の［切断／接続状況］→［PPTP］画面の［割当 IP アドレス］で確認できます。
送信ユーザ ID	user_pptpclnt （PPTPクライアントとしてのユーザID）
送信パスワード	pass_pptpclnt （PPTP クライアントとしてのパスワード）
認証プロトコル	MS-CHAPv2
接続モード	端末型接続
暗号化	MPPE-128

・［詳細設定］→［ルータ設定］→［LAN］

オプション	ip route 192.168.0.0/24/2 pptp xxx.xxx.xxx.xxx ※「xxx.xxx.xxx.xxx」は、サーバ側の本製品がPPPoE接続時にプロバイダから割り当てられたグローバルIPアドレスを指定します。 ※PPTPサーバ側のネットワーク番号とPPTPサーバのIPアドレスを結ぶIP経路情報を設定します。

操作

■サーバ側の接続

1. プロバイダ（接続相手先登録#0）に接続します。

■クライアント側の接続

1. プロバイダ（接続相手先登録#0）に接続します。

2. 接続相手先登録#1に設定した、PPTPサーバに接続します。

■PPTPでの通信を切断する

1. ［詳細設定］→［切断／接続状況］→［PPTP］をクリックします。
   ［切断／接続状況（PPTP）］画面が表示されます。

チャネル	PPTP1
接続状況	接続中(発信)
接続時刻	2003/09/20 16:16:22
相手先電話番号	192.168.1.233
接続モード	端末型
リンクプロトコル	LCP IPCP
相手先ルータアドレス	192.168.1.233
相手先DNSサーバアドレス	192.168.1.2
割り当てIPアドレス	192.168.0.35
無通信時間/自動切断時間(秒)	7/150
経過時間/最大接続時間(分)	0/180
チャネル	**PPTP2**
接続状況	空き

PPTPでの通信の状況を確認できます。

2. ［切断するチャネル］で、通信を切断したいPPTPのチャネルを選択します。

3. ［切断］ボタンをクリックします。

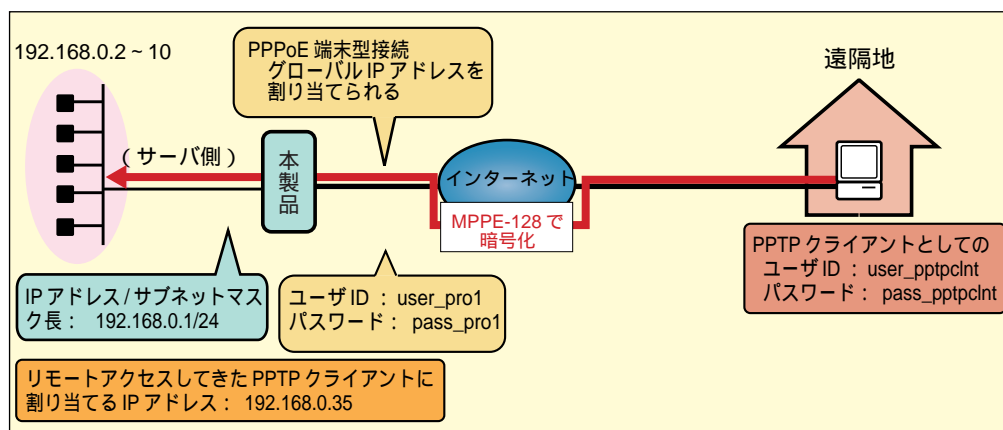
PPTPを使用した通信時は、通常より通信速度が遅くなることがあります。

◆ 本製品の暗号化について

本製品では、PPP通信での標準的な暗号化方式であるMPPE（Microsoft Point to Point Encryption）と、本製品独自の暗号化方式の2種類をサポートしています。
（本製品独自の暗号化方式については、「暗号化されたデータのやりとりをする」〈P.86〉を参照してください。）

MPPE-40	**暗号化にMPPEのキー長40bitを使用する場合に選択します。**
MPPE-128	**暗号化にMPPEのキー長128bitを使用する場合に選択します。**
MPPE-any	**通信相手の設定に合わせて、MPPE-40またはMPPE-128で暗号化するときに選択します。**

PPTPでWindowsのリモートアクセスを受け付ける

本製品はMPPEをサポートしているので、PPTP+MPPEを利用して遠隔地のWindowsマシンから本製品にダイヤルアップで接続できます。

PPTPを利用したVPNを構築するときは、本製品にグローバルIPアドレスが割り当てられている必要があります。プライベートIPアドレスを使用している一部のプロバイダでは、VPNを構築できない場合があります。あらかじめご了承ください。

設定ページ

■本製品側で設定する内容

●PPPoE端末型でプロバイダに接続するための設定

- ［詳細設定］ → ［接続／相手先登録］ → ［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user_pro1（プロバイダから通知されたユーザ ID）
送信パスワード	pass_pro1（プロバイダから通知されたパスワード）
通信チャネル	PPPoE（ランプ点灯）
接続モード	端末型接続

●PPTPサーバとしての設定

- ［詳細設定］→［接続／相手先登録］→［#8］

相手先電話番号	空欄にする（クライアントを特定しません。） ※ PPPoE 端末型接続時に、遠隔地のパソコンに割り当てられたグローバル IP アドレスを入力することもできます。
相手からの着信	［応じる］を選択
受信ユーザ ID	user_pptpclnt （PPTPクライアントが発信してくるユーザID）
受信パスワード	pass_pptpclnt （PPTPクライアントが発信してくるパスワード）
認証プロトコル	MS-CHAPv2
暗号化	MPPE-128

- ［詳細設定］→［ルータ設定］→［LAN］

リモートアクセスサーバ	［ON］を選択
リモート IP アドレス 1	192.168.0.35
オプション	ip filter 2 pass in * 192.168.0.1 tcp * pptp remote 0 ip filter 3 pass in * 192.168.0.1 gre * * remote 0 ip nat 2 192.168.0.1/tcp/pptp ipcp remote 0 ip nat 3 192.168.0.1/gre ipcp remote 0 ip nat 4 */*/* ipcp remote 0

パソコンの設定

PPTPを利用してリモートアクセスする場合は、Windowsの仮想プライベートネットワークの設定が必要です。

■Windows XPでVPNの設定をする

1. ［スタート］メニューの［コントロールパネル］をクリックします。

2. ［ネットワークとインターネット接続］→［ネットワーク接続］の順にクリックします。
   ［ネットワーク接続］ウィンドウが表示されます。

3. ［新しい接続を作成する］をクリックします。
   ［新しい接続ウィザードの開始］画面が表示されます。

4. ［次へ］ボタンをクリックします。

5. [職場のネットワークに接続する]をクリックして、[次へ]ボタンをクリックします。

6. [仮想プライベート ネットワーク接続]をクリックして、[次へ]ボタンをクリックします。

7. [会社名]に、このPPTP接続につける名前を入力します。わかりやすい名前であれば、何でも構いません。次に、[次へ]ボタンをクリックします。

8. [ホスト名またはIPアドレス]に、ダイヤルアップ接続するPPTPサーバのホスト名か、グローバルIPアドレスを入力します。
   本製品に割り当てられたグローバルIPアドレスは、サーバ側の[切断/接続状況]→[PPTP]画面の[割当てIPアドレス]で確認できます。
   次に、[次へ]ボタンをクリックします。

9. [完了]ボタンをクリックします。
   [会社名]に設定した名前の新しい接続のアイコンが表示されます。

■Windows XPで接続する

あらかじめプロバイダに接続してから、次の操作を行ってください。

1. [コントロールパネル]→[ネットワークとインターネット接続]→[ネットワーク接続]の順にクリックします。

2. 作成したVPN用の接続アイコンをダブルクリックします。
   [xxxxx(作成した接続名)への接続]ウィンドウが表示されます。

3. [ユーザ名]と[パスワード]に、サーバ側で設定しているPPTPクライアントとしてのユーザIDとパスワードを入力します。
   ユーザ名:user_pptpclnt
   パスワード:pass_pptpclnt

4. [プロパティ]ボタンをクリックします。

5. [全般]タブをクリックして、[宛先のホスト名またはIPアドレス]に、本製品(PPTPサーバ)に割り当てられているグローバルIPアドレスを入力します。

6. [セキュリティ]タブをクリックして、セキュリティオプションの[標準]が選択されていることを確認し、[データの暗号化を必ず要求する(データが暗号化されていない場合は切断する)]をチェックします。

7. [ネットワーク]タブをクリックし、[VPNの種類]で[自動]を選択して[設定]ボタンをクリックします。
   [PPPの設定]ダイアログが表示されます。

8. ［単一リンクに対してマルチリンクをネゴシエートする］にのみチェックを付けて、［OK］ボタンをクリックします。

9. プロパティダイアログの［OK］ボタンをクリックして、ダイアログを閉じます。

10. ［xxxxx（作成した接続名）への接続］ウィンドウで、［接続］ボタンをクリックします。
    本製品へのダイヤルアップ接続が開始されます。

■Windows 2000でVPNの設定をする

1. ［スタート］メニューの［コントロールパネル］をクリックします。

2. ［ネットワークとダイヤルアップ接続］をダブルクリックします。

3. ［新しい接続の作成］アイコンをダブルクリックします。
   ［ネットワークの接続ウィザードの開始］画面が表示されます。

4. ［次へ］ボタンをクリックします。

5. ［インターネット経由でプライベートネットワークに接続する］をクリックして、［次へ］ボタンをクリックします。

6. ［ホスト名またはIPアドレス］に、ダイヤルアップ接続するPPTPサーバのホスト名か、グローバルIPアドレスを入力します。
   本製品に割り当てられたグローバルIPアドレスは、サーバ側の［切断/接続状況］→［PPTP］画面の［割当てIPアドレス］で確認できます。
   ［次へ］ボタンをクリックします。

7. ［すべてのユーザー］または［自分のみ］をクリックして［次へ］ボタンをクリックします。

8. ［接続名］にこのPPTP接続につける名前を入力します。わかりやすい名前であれば、何でも構いません。次に、［完了］ボタンをクリックします。
   ［接続名］に設定した名前の新しい接続のアイコンが表示されます。

■Windows 2000でダイヤルアップ接続する

あらかじめプロバイダに接続してから、次の操作を行ってください。

1. ［コントロールパネル］→［ネットワークとダイヤルアップ接続］の順にクリックします。

2. 作成したVPN用の接続アイコンをダブルクリックします。
   ［xxxxx（作成した接続名）への接続］ウィンドウが表示されます。

3. ［ユーザ名］と［パスワード］に、サーバ側で設定しているPPTPクライアントとしてのユーザIDとパスワードを入力します。
   ユーザ名：user_pptpclnt
   パスワード：pass_pptpclnt

4. ［プロパティ］ボタンをクリックします。

5. ［ネットワーク］タブをクリックして、［宛先のホスト名またはIPアドレス］に、本製品（PPTPサーバ）に割り当てられているグローバルIPアドレスを入力します。

6. ［セキュリティ］タブをクリックして、セキュリティオプションの［標準］が選択されていることを確認し、［データの暗号化を必ず要求する（データが暗号化されていない場合は切断する)］をチェックします。

7. ［ネットワーク］タブをクリックし、［呼び出すVPNサーバーの種類］で［自動］を選択して［設定］ボタンをクリックします。
   ［PPPの設定］ダイアログが表示されます。

8. ［単一リンクに対してマルチリンクをネゴシエートする］にのみチェックを付けて、［OK］ボタンをクリックします。

9. プロパティダイアログの［OK］ボタンをクリックして、ダイアログを閉じます。

10. ［xxxxx（作成した接続名）への接続］ウィンドウで、［接続］ボタンをクリックします。
   本製品への接続が開始されます。

■Windows 98 SE/MeでVPNの設定をする

Windows98 SE/Meの場合は、仮想プライベートネットワークが必要です。お使いのパソコンにインストールされていない場合は、まずインストールを行います。WindowsのCD-ROMを用意してください。

●仮想プライベートネットワークのインストール

1. ［スタート］メニューの［コントロールパネル］をクリックします。

2. ［ネットワークとダイヤルアップ接続］をダブルクリックします。

3. ［アプリケーションの追加と削除アイコンをダブルクリックし、［Windowsファイル］タブをクリックします。

4. ［通信］をクリックし、［詳細］ボタンをクリックします。

5. ［仮想プライベートネットワーク］［ダイヤルアップネットワーク］をチェックして、［OK］ボタンをクリックします。

   以降は、Windowsの画面の指示に従って、インストール作業を続けてください。

6. インストールが終了したら、パソコンを再起動します。

●VPNの設定を行う

1. ［マイコンピュータ］の［ダイヤルアップネットワーク］をダブルクリックし、［新しい接続］をダブルクリックします。

2. ［接続名］にこのPPTP接続につける名前を入力します。わかりやすい名前であれば、何でも構いません。次に［モデムの選択］から［Microsoft VPN Adapter］を選択し、［次へ］ボタンをクリックします。

3. ［ホスト名またはIPアドレス］に、ダイヤルアップ接続するPPTPサーバのホスト名か、グローバルIPアドレスを入力します。

   本製品に割り当てられたグローバルIPアドレスは、サーバ側の［切断/接続状況］→［PPTP］画面の［割当てIPアドレス］で確認できます。
   次に、［次へ］ボタンをクリックします。

4. 接続名を確認してから、［完了］ボタンをクリックします。

   ［接続名］に設定した名前の新しい接続のアイコンが表示されます。

5. 新しいアイコンを右ボタンをクリックし、表示されたメニューから［プロパティ］を選択します。

6. Windows Meの場合は［ネットワーク］タブを、Windows 98SEの場合は［サーバーの種類］タブをクリックします。

7. 次の設定を行います。

   ・Windows Meの場合
   ［TCP/IP］のみチェックし、［OK］ボタンをクリックします。

   ・Windows 98 SEの場合
   ［詳細オプション］で、［暗号化パスワードを使う］［データの暗号化を使用する］のみチェックします。
   ［使用できるネットワークプロトコル］で、［TCP/IP］のみチェックします。
   次に［OK］ボタンをクリックすると、Windows 98SEの場合は設定が終了です。

8. Windows Meの場合は、［セキュリティ］タブをクリックして、［暗号化パスワードを使う］［データの暗号化が必要］をチェックし、［OK］ボタンをクリックします。以上でWindows Meでの設定が終了です。

■Windows 98 SE/Meでダイヤルアップ接続する

あらかじめプロバイダに接続してから、次の操作を行ってください。

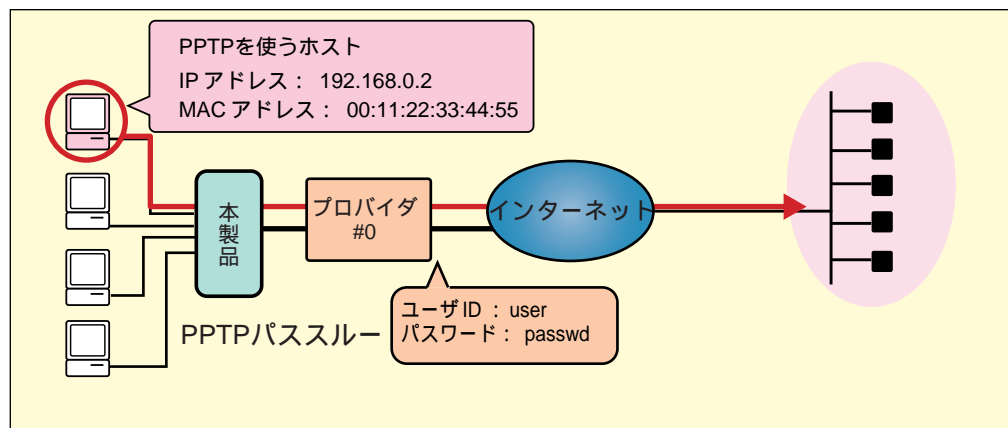
1. ［マイコンピュータ］→［ダイヤルアップネットワーク］の順にダブルクリックします。

2. 作成したVPN用の接続アイコンをダブルクリックします。
   ［接続］ウィンドウが表示されます。

3. ［ユーザ名］と［パスワード］に、サーバ側で設定しているPPTPクライアントとしてのユーザIDとパスワードを入力します。
   ユーザ名：user_pptpclnt
   パスワード：pass_pptpclnt

4. ［接続］ウィンドウで、［接続］ボタンをクリックします。
   本製品への接続が開始されます。

VPNパススルー

本製品は、VPNのプロトコルをIPアドレス（変換）テーブルを作成しなくても自動的に設定して通過させることができる、「VPNパススルー」機能を搭載しています。本製品は、IPsec、PPTP、L2TPの3種類のプロトコルに対応しています。
ここでは、PPPoE端末型でインターネットに接続し、LAN内の特定のパソコンでPPTPで通信を行う場合の設定を解説します。

設定ページ

■プロバイダに接続するための設定

● ［詳細設定］ → ［接続／相手先登録］ → ［#0］

相手先名称	名称（何でも構いません）を設定
送信ユーザ ID	user
送信パスワード	passwd
通信チャネル	［PPPoE（ランプ点灯）］を選択
接続モード	［端末型接続］を選択

■VPNパススルーの設定

● ［詳細設定］ → ［セキュリティ］

PPTP パススルー	［透過する］を選択
LAN 側 PPTP ホストアドレス	192.168.0.2

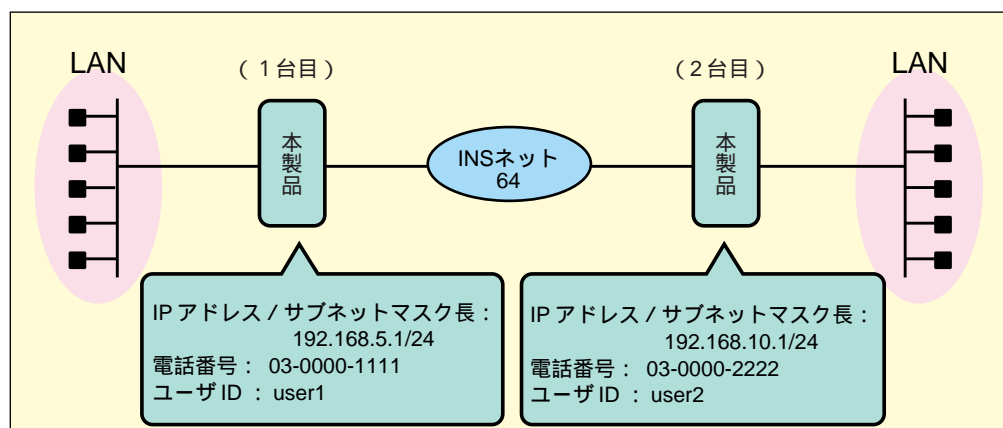
● ［詳細設定］ → ［ルータ設定］ → ［LAN］

オプション	ip host 192.168.0.2 user1.mn128soho.co.jp 00:11:22:33:44:55 （user1.mn128soho.co.jp：任意のホスト名を割り当てます。） （00:11:22:33:44:55：パソコンのMACアドレスです。）

LAN上にVPNのサーバを設置する場合は、［LAN側のホストアドレス］を必ず設定してください。なお、LAN側のホストアドレスを設定すると、そのIPアドレスのパソコン以外は、VPN（IPsec、PPTP、L2TP）による通信ができません。

LAN側のホストアドレスを指定しなかった場合は、LAN内の複数のパソコンでVPN（IPsec、PPTP、L2TP）による通信が可能になります。ただし、同一相手先へ同時に接続することはできません。また、この場合、インターネット側から接続を開始することはできません。

本製品同士でネットワーク接続する ISDN

本製品同士を接続してLAN間接続する場合、異なるサブネットワークアドレスのIPアドレスを設定する必要があります。

設定ページ

■［詳細設定］→［接続／相手先登録］→［#0］

設定する項目	1台目	2台目
相手先名称	2台目の名称（何でも構いません）	1台目の名称（何でも構いません）
相手先電話番号	03-0000-2222 ※発信者番号の通知が必要です。	03-0000-1111 ※発信者番号の通知が必要です。
送信ユーザID	user1	user2
接続モード	［LAN 型接続］を選択	［LAN 型接続］を選択
相手からの着信	［応じる］を選択	［応じる］を選択
受信ユーザID	user2	user1

■［詳細設定］→［ルータ設定］→［LAN］

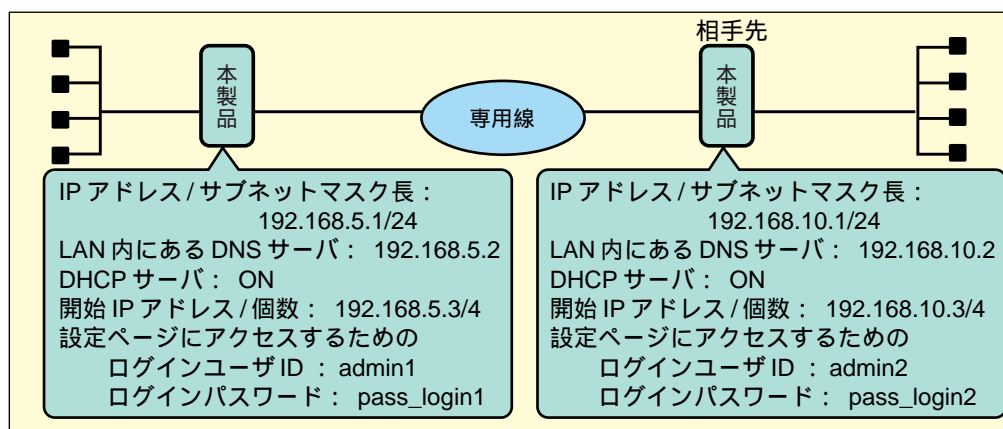
設定する項目	1台目	2台目
本体のIPアドレス/サブネットマスク長	192.168.5.1/24	192.168.10.1/24

■［詳細設定］→［セキュリティ設定］

設定する項目	1台目	2台目
SPI	OFF	OFF

上記の設定をしても接続できない場合は、「困ったときは」の「本製品同士で接続できない」〈P.123〉を参照してください。

本製品同士で専用線ネットワーク接続する

本製品同士（またはMN128-SOHOシリーズ）を専用線で接続する場合、購入時の設定のままでは同じサブネットワーク番号のIPアドレスが設定されているため、接続することができません。異なるサブネットワークアドレスのIPアドレスを設定します。

設定ページ

■ [詳細設定] → [接続／相手先登録] → [#0]

設定する項目	1 台目	2 台目
DNSサーバアドレス	192.168.5.2	192.168.10.2

■ [詳細設定] → [ルータ設定] → [LAN]

設定する項目	1台目	2台目
本体のIPアドレス/サブネットマスク長	192.168.5.1/24	192.168.10.1/24
DHCPサーバ機能	ON	ON
開始IPアドレス/個数	192.168.5.3/4	192.168.10.3/4

■ [詳細設定] → [ルータ設定] → [ISDN]

設定する項目	1 台目	2 台目
回線種別	専用線128Kbps	専用線128Kbps

■［詳細設定］→［セキュリティ設定］

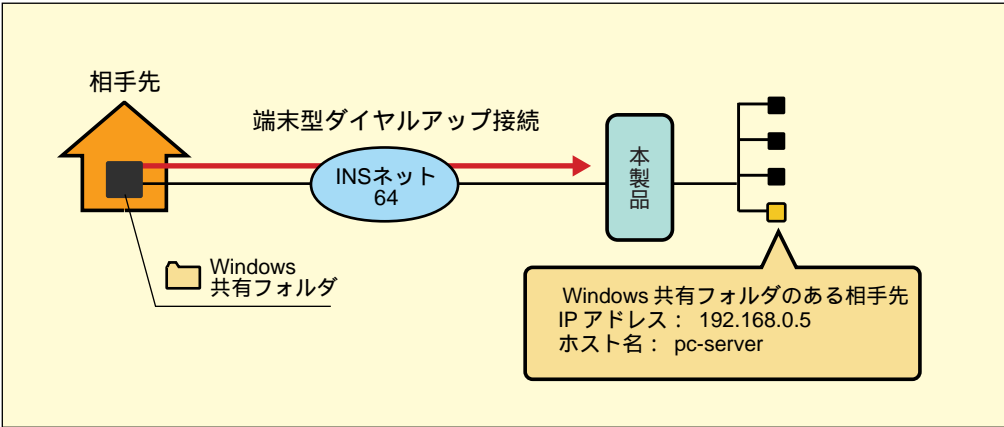
設定する項目	1台目	2台目
SPI	OFF	OFF

■［詳細設定］→［管理コマンド・設定］→［ユーザ・パスワード変更］

専用線で接続する場合は、セキュリティのため設定ページにユーザIDとパスワードを設定しておきます。

設定する項目	1台目	2台目
ユーザID	admin1 ※設定ページにアクセスするためのユーザIDを入力	admin2 ※設定ページにアクセスするためのユーザIDを入力
パスワード	pass_login1 ※設定ページにアクセスするためのパスワードを入力	pass_login2 ※設定ページにアクセスするためのパスワードを入力
パスワード（再入力）	pass_login1	pass_login2

Windows間で共有フォルダを利用する

相手先との接続中に、WindowsのMicrosoftネットワークを使って、相手先の共有フォルダを利用したいときは、パソコンの「LMHOSTS」ファイル（テキストファイル形式のデータベースファイル）に設定を保存してください。

パソコンの設定

1. パソコンで、「LMHOSTS.SAM」ファイル（サンプルファイル）を探します。
「LMHOSTS.SAM」ファイルは、次のフォルダの中にあります。

Windows XP	C:\WINDOWS→［SYSTEM32］→［DRIVERS］→［ETC］フォルダ
Windows 2000	C:\WINDOWS→［SYSTEM32］→［DRIVERS］→［ETC］フォルダ
Windows 98 SE/Me	C:\WINDOWS

2. 「LMHOSTS.SAM」ファイルを「LMHOSTS」という名前で保存し直します（拡張子はつけません）。
「LMHOSTS.SAM」ファイルと同じディレクトリに「LMHOSTS」という名前のファイルがすでに存在するときは、そのファイルを使用します。別名で保存し直す必要はありません。

3. テキストエディタなどを起動し、「LMHOSTS」ファイルを開きます。

4. 「LMHOSTS」ファイルに、相手先のパソコンのIPアドレスとホスト名の組み合わせを登録します。

書式：［IPアドレス］［ホスト名］ #PRE
192.168.0.5　pc-server #pre
IPアドレスとホスト名は半角スペース、またはタブで区切ります。
IPアドレスとホスト名の組み合わせを複数登録するときは、組み合わせを1組みずつ改行してください。

5. 上書き保存します。

相手先の共有フォルダを利用するときは、相手先に回線を接続後、パソコンの「マイネットワーク」（ネットワークコンピュータ）のアイコンをダブルクリックします。開いたウィンドウに、相手先のパソコンのアイコンが表示されます。

◆別の方法を使って、Windows間で共有フォルダを利用するには
「LMHOSTS」ファイルを修正しても相手先のパソコンのアイコンが表示されないときは、パソコンでエクスプローラを起動し、次のいずれかの操作を行ってください。

（1）コンピュータの検索

1. ［ツール］メニュー→［検索］→［ほかのコンピュータ］を選択します。
   ［検索コンピュータ］画面が表示されます。
2. ［名前］に利用したい相手先のパソコンのホスト名を入力します。
3. ［検索開始］ボタンをクリックします。

（2）ネットワークドライブを割り当てる

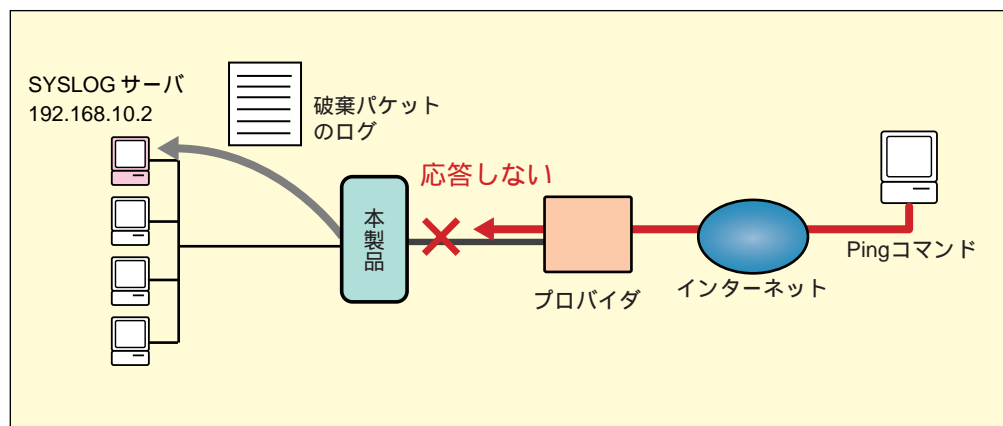
1. ［ツール］メニュー→［ネットワークドライブの割り当て］を選択します。
   ［ネットワークドライブの割り当て］画面が表示されます。
2. 次の項目を設定します。
   ［ドライブ］→割り当てるドライブ番号を入力
   ［パス］→利用したいパソコンまでのパスを入力
3. ［OK］ボタンをクリックします。

本製品には、LAN上にWindows XP/2000（2000 Server）/98 SE/Meがあるときに発生する「意図しない自動接続」を防止するためのフィルタが工場出荷時の状態で設定されています。このため、Microsoftネットワークにアクセスしただけでは、相手先に自動接続しません。なお、購入時に登録されているフィルタを削除すると、意図しない自動接続が行われてしまうことがあるので、ご注意ください。

7 ルータ機能のセキュリティ

本製品には、セキュリティ対策の機能として「ステルスモード」「SPI」「IPフィルタ」「暗号化」機能が用意されています。ただし、これらの機能を使用していても、絶対に被害に遭わないということはありません。十分にご注意ください。

ステルスモードにする

ステルスモードにすると、インターネットからPINGコマンドに応答しなくなり、またインターネットへのICMPエラーやTCPのリセットを返さなくります（ポート113を除く）。これにより、外部に本製品の存在を隠すことができ、ポートスキャンなどの攻撃から守ることができます。応答せずに破棄したパケットのログをSYSLOGサーバに出力可能です。

設定ページ

■［詳細設定］→［セキュリティ設定］

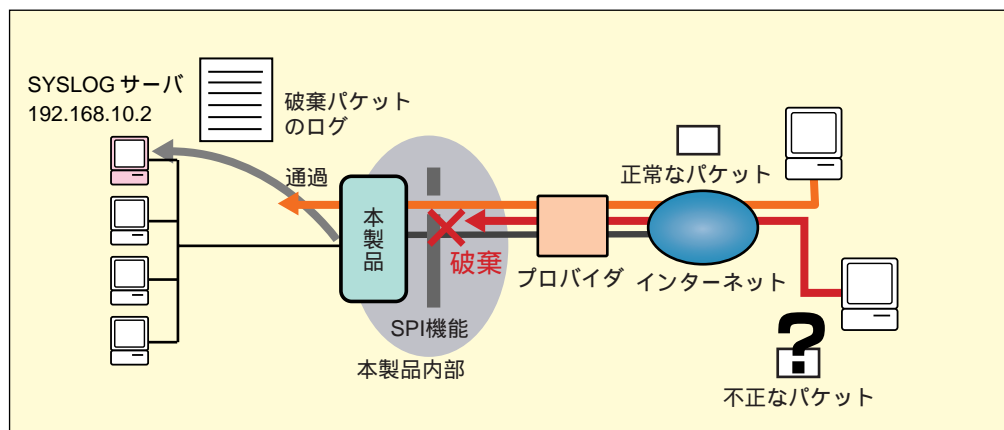
ステルスモード	ON
ログ出力	する

■［詳細設定］→［ルータ設定］→［LAN］

SYSLOG 機能	［NOTICE］をチェック
SYSLOG ホストアドレス	192.168.10.2
SYSLOG ファシリティ	1

※SYSLOG機能に関しては、「SYSLOGサーバに出力する」〈P.112〉を参照してください。

SPI機能を使う

「SPI（ステートフル・パケット・インスペクション）」とは、受信したパケットの内容や通信の状態を監視して、自動的にポートの開放・閉鎖を行う機能です。SPI機能を使うと、不正な手段で送信されたパケットを破棄することができます。

設定ページ

■［詳細設定］→［セキュリティ設定］

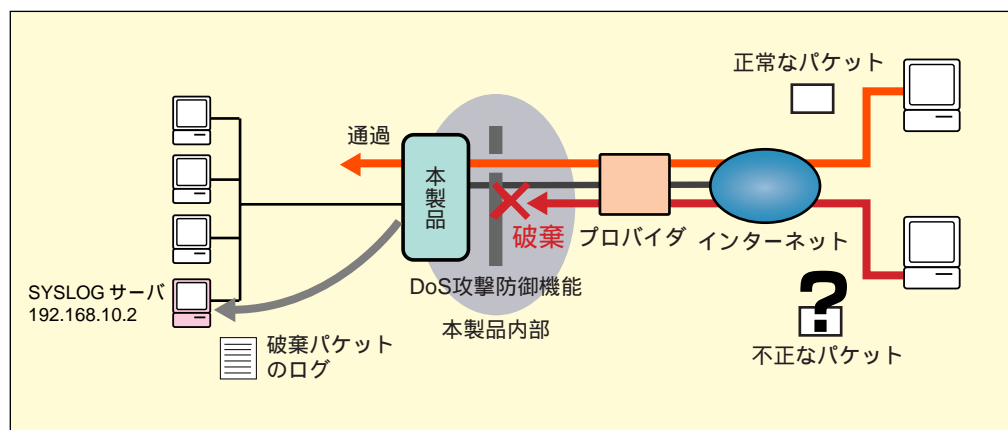
SPI	ON
ログ出力	する

■［詳細設定］→［ルータ設定］→［LAN］

SYSLOG 機能	［NOTICE］をチェック
SYSLOG ホストアドレス	192.168.10.2
SYSLOG ファシリティ	1

※SYSLOG機能に関しては、「SYSLOGサーバに出力する」〈P.112〉を参照してください。

DoS攻撃防御機能を利用する

DoS攻撃（Denial of Service攻撃）とは、ネットワークを通じて不正なデータを送信したり、大量にデータ送信したりすることにより、相手のサービスを使用不能にすることです。
本製品では、DoS攻撃防御機能を利用することによって不正なアクセスを検知し、本製品およびLAN側のネットワークを保護することができます。また、DoS攻撃を検知したら、LANの管理者など指定した相手先へメールを送信して通知できます。
※導入時の設定では、DoS攻撃防御機能はオフになっています。

■本製品で防御するDoS攻撃について

●FIN Scan

TCP FINフラグがオンになっているパケットを送信して、ポートをスキャンします。本製品ではTCP通信を監視し、パケットのFINフラグが不正にオンになっているパケットを破棄します。

●Null Scan

TCPフラグをすべてオフにしたパケットを送信して、ポートをスキャンします。本製品では、パケットのフラグをチェックし、すべてオフになっているパケットを破棄します。

●Xmas Scan（Nmap Xmas Scan）

URG、PSH、FINフラグがすべてオンのパケットを送信し、ポートをスキャンします。本製品では、上記のフラグをチェックし、すべてオンになっているパケットを破棄します。

●Smurf攻撃

送信元アドレスを偽造したICMP echo requestパケットをブロードキャストすることにより、大量のICMP echo replyパケットを、相手先に返送させるという仕組みの攻撃です。本製品では、ブロードキャストアドレス宛てのICMP echo requestパケットを破棄します。また、IPアドレスが、本製品のサブネットと同じかどうかをチェックして、同じである場合、偽造アドレスとみなし、そのパケットを破棄します。

●Ping of Death攻撃

Pingコマンドを使って不正なサイズのIPパケットを送信することにより、相手先の処理を不能にする攻撃です。本製品では、IPパケットのサイズをチェックして、不正なサイズのパケット

を破棄します。

●Teardrop攻撃

断片化されたIPパケット（IPフラグメンテーションパケット）を再構築する際の、TCP/IPの実装上の問題に対する攻撃です。IPフラグメンテーションパケットには、再構築時に使用されるオフセット情報が含まれますが、そのオフセット情報を偽造することで、相手先の処理を不能にします。本製品では、オフセット情報をチェックし、同じオフセット番号のパケットを破棄することにより、そのIPアドレスからのセッションを遮断します。

●IP Spoofing攻撃

送信元のIPアドレスを、相手先のIPアドレスに偽装することによる攻撃です。本製品では、送信元のIPアドレスをチェックし、プライベートIPアドレスの場合、そのパケットを破棄します。

●Land攻撃

送信元と送信先に同じIPアドレスを持つパケットを相手先に送信することにより、相手先のパフォーマンスを低下させたり、処理不能にしたりする攻撃です。
本製品では、送信元と送信先のアドレスが同一かどうかをチェックし、同一のパケットを破棄します。

●IP with Zero Length攻撃

IPパケットの最初のフラグメンテーションに、長さゼロのパケットを「おとり」として送信し、その後悪影響を及ぼすパケットを送り込むことで、相手先を攻撃します。
本製品では、パケットの最初のフラグメンテーションの長さ情報チェックし、ゼロの場合、そのパケットを破棄します。

●Fraggle（UDP loop）

送信元のIPアドレスを偽造し、UDPのecho requestパケットをブロードキャストすることにより、相手先のパフォーマンスを低下させたり、処理不能にしたりする攻撃です。Echo、Chargen、Daytime、Qotdの各ポートが利用されます。
本製品では、ブロードキャストアドレス宛てのUDP echo requestパケットを破棄します。また、送信元のIPアドレスが、本製品のサブネットと同じかどうかをチェックして、同じである場合、偽造アドレスとみなし、そのパケットを破棄します。また、送信元と送信先のポート番号が、7（Echo）、19（Chargen）、13（Daytime）、17（Qotd）の組み合わせである場合、そのパケットを破棄します。

●Snork攻撃

送信先ポート番号が135、送信元ポート番号が7（Echo）、19（Chargen）、13（Daytime）、135のいずれかのUDPパケットを送信し、不正に処理を繰り返させる攻撃です。本製品では、このようなパケットをすべて破棄します。

●リロード攻撃

Webページを連続してリロードすることにより、相手先に負荷を与える攻撃です。
本製品では、確立されたセッション数をカウントし、上限値を超えると、そのIPアドレスからのセッションを遮断します。

●Fragment Flood

断片化されたパケットを大量に送信することにより、相手先を処理不能にする攻撃です。本製品では、送信元のIPアドレスごとに、断片化されたパケット数をカウントし、設定した上限値を超えると、そのIPアドレスからのセッションを遮断します。

●Connection Flood

長時間オープン状態にし続けることにより、相手先のソケットを占拠する攻撃です。本製品では、一定時間アイドル状態のまま確立されたセッション数をカウントし、上限値を超えると、そのIPアドレスからのセッションを遮断します。

●Ping Flooding

大量のICMP echo requestパケットを送信し、相手先のパフォーマンスを低下させる攻撃です。
本製品では、ICMP echo requestパケット数をカウントし、設定した上限値を超えるとそのIPアドレスからのICMP echo requestパケットを破棄します。

●SYN Flood

SYNフラグがオンになっているTCPパケットを連続的に送信することにより、ハーフオープン状態のセッションを増加させ、相手先を処理不能にする攻撃です。
本製品では、SYNフラグがオンになっているTCPパケットの数、およびハーフオープン状態のセッション数をカウントし、設定した上限値を超えるとそのパケットを破棄します。

設定ページ

■［詳細設定］→［セキュリティ設定］

DoS 攻撃防御		する
ログ出力		する
メール通知機能	送信先メールアドレス	address1@xxxx.ne.jp
	送信元メールアドレス	address2@yyyy.ne.jp
	メール（SMTP）サーバ	172.16.15.100 ※ SMTP サーバの IP アドレス、またはドメイン名を入力します。

［DoS攻撃防御設定］の［DoS攻撃防御］で［する］を選択すると、以下のDoS攻撃が防御されます。

- FIN Scan
- Smurf攻撃
- IP Spoofing攻撃
- Fraggle（UDP loop）
- Fragment Flood
- Ping Flooding
- Null Scan
- Ping of Death攻撃
- Land攻撃
- Snork攻撃
- Connection Flood
- SYN Flood
- Xmas Scan（Nmap Xmas Scan）
- Teardrop攻撃
- IP with Zero Length攻撃
- リロード攻撃

■［詳細設定］→［ルータ設定］→［LAN］

SYSLOGサーバを設定します。

SYSLOG 機能	［NOTICE］をチェック
SYSLOG ホストアドレス	192.168.10.2
SYSLOG ファシリティ	1

※SYSLOG機能に関しては、「SYSLOGサーバに出力する」〈P.112〉を参照してください。

● プライベートアドレスのネットワークを接続する場合

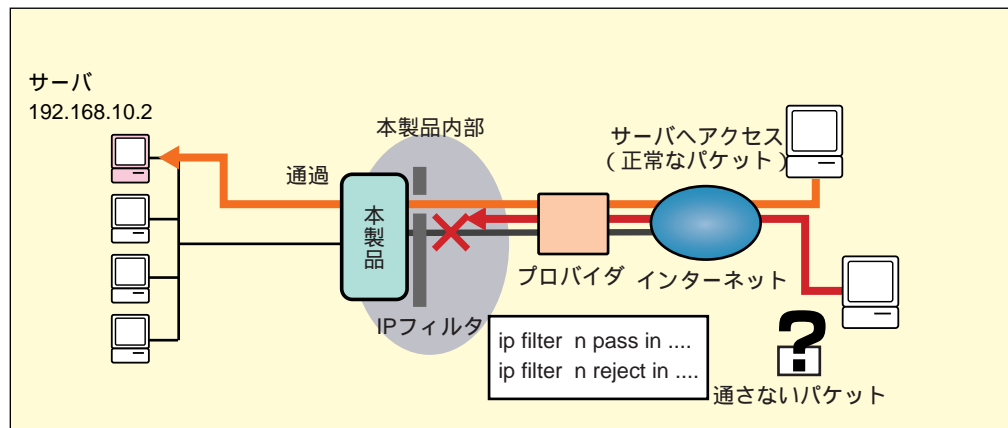
DoS攻撃防御をオンにすると、IP Spoofing攻撃防御の機能がオンになり、送信元のIPアドレスがプライベートアドレスのパケットが破棄されます。そのため、以下のような通信ができなくなる場合があります。

- 2拠点のプライベートアドレスネットワークをLAN型で接続する場合
- 本製品のLAN側で使用しているIPアドレスがプライベートアドレスで、リモートアクセスを受ける場合

この場合、該当する接続相手先のDoS攻撃防御の設定をオフにすると通信できるようになります。

接続相手先のDoS攻撃防御をオフにしたいときは、［詳細設定］→［セキュリティ設定］→［接続/相手先登録］→［DoS攻撃防御設定］の［DoS攻撃防御］で［しない］を設定してください。

IPフィルタの設定

IPフィルタは、送信元や送信先、ポート番号、通信の方向などの条件を設定して、本製品に送られてきたパケットを通過させるか拒否するかを判断する機能です。LAN側からインターネットへの意図しない接続を防ぐ設定もできます。

FTTH、ADSL、CATV、フレッツ・ISDNなど、常時インターネットできる環境では、外部からの不正アクセスや攻撃にさらされる危険性も高くなります。IPフィルタ機能を使って、LAN内に通す・通さないパケットを指定して、セキュリティ対策を十分に行う必要があります。

本製品には、工場出荷時の設定でいくつかのフィルタが設定されているほか、クイック設定を行うと、自動的にフィルタが設定されます。詳しくは、「クイック設定で自動的に設定されるフィルタ」〈P.137〉をお読みください。

IPフィルタは、設定ページの［詳細設定］→［ルータ設定］→［LAN］画面の［オプション］欄にコマンドを次の書式で入力することで設定できます。

ip filter {fnumber type dir srcaddr dstaddr protocol srcport dsport interface [rnumber] [log]}

fnumber		フィルタ番号 1～64の間で設定します。 番号の小さい方の設定が優先されます。
type	 pass reject restrict	フィルタのタイプ 一致すればパケットを通す 一致すればパケットを破棄する 回線が接続されている場合だけパケットを通す
dir	 in out	方向 受信時にフィルタリングする 送信時にフィルタリングする
srcaddr		送信元アドレス［/ネットマスク¦-範囲指定］ 「*」を入力するとすべてのIPアドレスが対象になります。 範囲を指定するときは、「-」で入力します。
dstaddr		送信先アドレス［/ネットマスク¦-範囲指定］ 「*」を入力するとすべてのIPアドレスが対象になります。 範囲を指定するときは、「-」で入力します。
protocol	 ニーモニック	プロトコル番号、またはニーモニック 「*」を入力するとすべてが対象になります。 範囲を指定するときは、「-」で入力します。 esp、gre、icmp、ipencap、tcp、tcpest、tcpfin、udp tcpestはSYN、tcpfinはFIN/RSTパケットを対象とします。
srcport	 ニーモニック	送信元ポート番号、またはニーモニック 「*」を入力するとすべてが対象になります。 範囲を指定するときは、「-」で入力します。 ftp、ftpdata、telnet、smtp、www、pop3、sunrpc nntp、ntp、login、pptp、domain、route、who
dstport		送信先ポート番号、またはニーモニック 「*」を入力するとすべてが対象になります。 範囲を指定するときは、「-」で入力します。
interface	local remote wanether wanany	LAN側のフィルタ WAN側（接続相手-ISDN、PPTP、PPPoE）のフィルタ WAN側（DHCPサーバからのアドレス取得、手動による固定IPアドレスの設定）のフィルタ すべてのWAN側のフィルタ
rnumber		相手先番号 1～15で指定します。 remoteの場合は、「*」ですべての相手先を指定できます。
log	 nolog	ログタイプ SYSLOGサーバにログを出力しない

設定ページ

■［詳細設定］→［ルータ設定］→［LAN］

●相手先#1から「192.168.0.2」のFTPサーバだけのアクセスを許可する

オプション	ip filter 1 pass in * 192.168.0.2/32 tcp * ftpdata-ftp remote1 ip filter 2 reject in * * * * * remote1

●WWWでのアクセスを許可する

オプション	ip filter 1 pass in * 192.168.0.2/32 tcp * www remote1

本製品のIPフィルタ機能は、番号の小さい順から参照して条件に一致したものから処理していきます。内容によっては設定順を間違えると、フィルタが無効になるので注意してください。たとえば、「インターネット側からのTCPアクセスをすべて禁止する」フィルタが上位に設定されている場合、その下に特定のTCPパケットを通す設定をしても有効にはなりません。

次のような例では、フィルタ58ですべてのTCPパケットが破棄されるので、フィルタ59を設定してもインターネット側からWWWサーバにアクセスすることはできません。

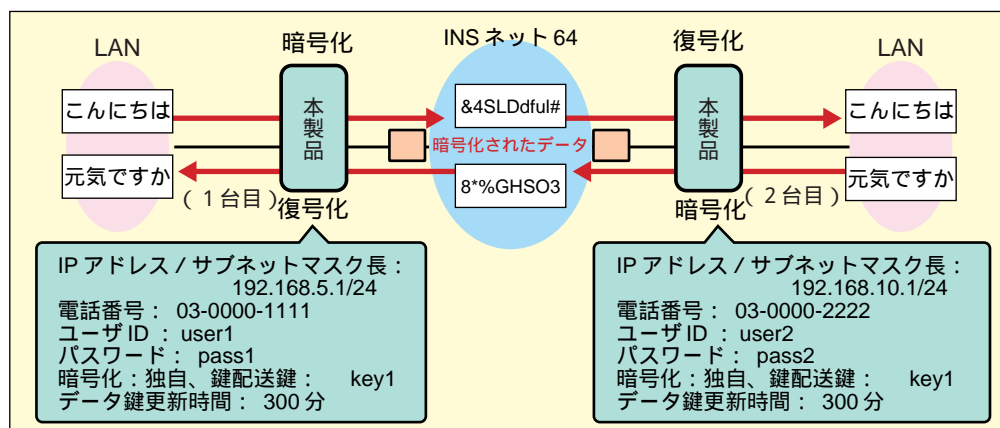
オプション	ip filter 58 reject in * * tcpest * * remote 1 （インターネット側から LAN 内への TCP アクセスを禁止） ip filter 59 pass in * 192.168.0.2/32 tcp * www remote 1 （「192.168.0.2」宛ての www パケットを通す）

次のようにフィルタの順序を逆にすると、フィルタ58で「192.168.0.2」宛てのwwwパケットを通し、フィルタ59でそれ以外のTCPパケットを破棄するようになります。

オプション	ip filter 58 pass in * 192.168.0.2/32 tcp * www remote 1 （「192.168.0.2」宛ての www パケットを通す） ip filter 59 reject in * * tcpest * * remote 1 （インターネット側から LAN 内への TCP アクセスを禁止）

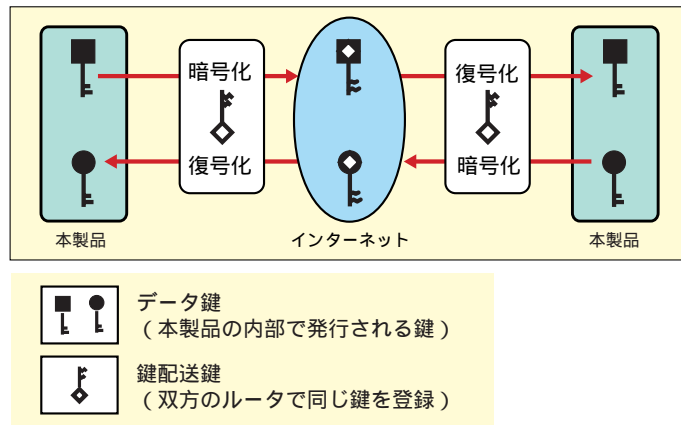
フィルタの登録順位は、先に条件を限定しているフィルタ、最後に条件を広範囲にしているフィルタに設定します。
インターネット側から受け取ったパケットの処理は、基本は「reject in（破棄）」、必要なものだけ「pass in（受信）」と考えるとよいでしょう。

暗号化されたデータのやりとりをする

本製品は、PPPでの通信中MPPE暗号化方式のほか、本製品同士（またはMN128-SOHOシリーズ、MN128-R）を接続する場合は独自の方式でデータを暗号化できます。

暗号化されたデータをやりとりができるのは、次の方法で通信した場合のみです。
- PPPoEでインターネットにアクセスし、PPP通信するとき
- INSネット64を利用してPPP通信するとき
- PPTP接続してPPP通信するとき

暗号化すると、「鍵」と呼ばれる秘密の情報を用いて、元のデータを一見意味のないデータに変換（暗号化）してネットワークに流すことができます。送信側と受信側以外の第３者からは、元のデータがわからないように保護できます。受信側は、「鍵」を元にしてデータを復元（復合化）することで、送信側からの情報を正しく受信することができます。暗号化には、2種類の鍵を使います。一方を鍵配送鍵、もう一方をデータ鍵と呼びます。鍵配送鍵は、あらかじめ設定しておく必要がありますが、データ鍵は自動的に本製品の内部で発行されます。

暗号化したデータをやり取りするためには、まず双方の本製品に同じ鍵配送鍵登録します。そうすると、接続時に鍵配送鍵で暗号化されたデータ鍵をお互いに送信するので、受け取ったデータ鍵を鍵配送鍵で復号化し、お互いに相手のデータ鍵を手に入れます。以降、送信側はデータ鍵を使ってデータを暗号化し、受信側は相手のデータ鍵を使って復号化します。

暗号化されたデータをやりとりするときは、通常より通信速度が遅くなることがあります。

データ鍵は、接続するたびに新しく発行されます。また、PPP接続後、一定時間ごとにデータ鍵を変更することを相手側に要求できます。

設定ページ

■［詳細設定］→［接続相手先登録］→［#0］

設定する項目	1台目	2台目
相手先名称	2台目の名称 （何でも構いません）	1台目の名称 （何でも構いません）
相手先電話番号	03-0000-2222 ※発信者番号の通知が必要です。	03-0000-1111 ※発信者番号の通知が必要です。
送信ユーザ ID	user1	user2
送信パスワード	pass1	pass2
接続モード	［LAN 型接続］を選択	［LAN 型接続］を選択
相手からの着信	［応じる］を選択	［応じる］を選択
受信ユーザ ID	user2	user1
受信パスワード	pass2	pass1
暗号化	［独自］を選択	［独自］を選択
鍵配送鍵	key1	key1
データ鍵更新時間	300 分	300 分

※［鍵配送鍵］は、双方の本製品で同じ文字列を入力します。なお、セキュリティのため［鍵配送鍵］の設定は、定期的に変更することをお勧めします。

■［詳細設定］→［ルータ設定］→［LAN］

設定する項目	1台目	2台目
本体のIPアドレス/ サブネットマスク長	192.168.5.1/24	192.168.10.1/24

無線LANを安全に使うポイント

■無線LANのセキュリティ問題について

無線LANは、配線や特別な設定なしにすべてのパソコンや機器が相互に通信ができるように設計されています。反面、セキュリティの設定をしないと、無線LANの電波が届く範囲内であれば誰でも簡単に、通信内容を傍受、あるいはネットワークに侵入することが可能になるという問題があります。無線LANをお使いの場合は、有線のLAN以上にセキュリティ対策を十分に行うことをお勧めします。

■無線LANのセキュリティ機能の種類

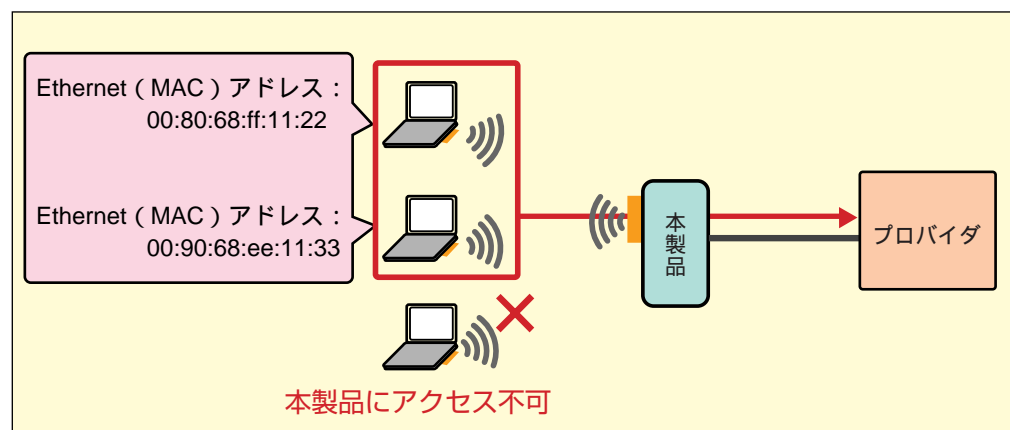
上記の問題を防ぐため、本製品ではIEEE802.11方式の無線LANでは設定できる次のセキュリティ機能を搭載しています。第三者が簡単に盗聴・侵入できないようにするために、セキュリティの設定は必ず行ってください。

セキュリティ機能	概要
SSID（Service Set Identifier）	パソコンが接続先である本製品を指定する ID で、同じ SSID を設定したパソコンだけが本製品に接続できます。
無線ステルス	SSID が空白、または「ANY」に設定されているパソコンからは本製品にアクセスできないように設定できます。この場合、SSID をほかのパソコンから検索できなくなります。
WEP （Wired Equivalent Privacy）	共通の暗号化キー（WEP キー）で本製品とパソコン間のデータを暗号化します。
WPA-PSK	WPA 共有キーを使用して、認証・暗号化を行います。暗号化方式には、「TKIP」「AES」のどちらかを使用します。WEP よりもさらにセキュリティが強化されています。WEP と同時に設定することはできません。
MAC アドレスフィルタリング	無線 LAN で使うパソコンの MAC アドレスを本製品にあらかじめ登録しておき、登録されているパソコンだけを接続可能にします。

※IEEE802.11g対応の無線LANカードを使う場合には、チャネルを14に設定しても13に変更されます。

接続できるパソコンを制限する

無線で本製品に接続できるパソコンを限定するときは、相手のパソコンのMACアドレスを登録します。MACアドレスを登録すると、それ以外のパソコンとは通信できません。これにより、意図しない第三者が勝手に本製品を利用するのを防ぐことができます。

登録したMACアドレスを持つパソコン以外が、本製品に接続するのを禁止する機能です。外部からの侵入を防ぐことができますが、盗聴防止には効果はありません。また専用のツールでMACアドレスを盗聴される可能性があり、WEPとあわせて使用することを推奨します。

設定ページ

■［詳細設定］→［PCカード設定］→［無線カード］

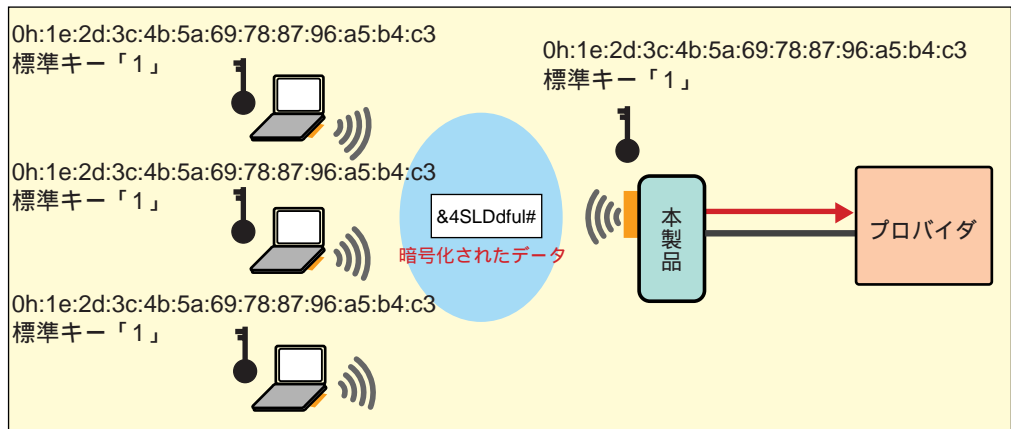
オプション	card air11 node 00:80:68:ff:11:22 card air11 node 00:90:68:ee:11:33 ※ 32 件まで登録できます。

◆パソコンに取り付けた無線LANカードのMACアドレスを確認する

各パソコンでMACアドレスを確認できます。操作方法は「パソコンのMACアドレスを確認する」〈P.25〉を参照してください。

無線LANの通信を暗号化する（WEPを使用する）

WEPを利用して無線データを暗号化することで、無線LANのセキュリティを強化することができます。
本製品では、IEEE802.11b規格（64bit、128bitキー）と、IEEE802.11g（64bit、128bit、152bit）のWEPキーに対応しています。お使いの無線LANカードの規格を確認してください。
不正な解読を困難にするために、128bitまたは152bitのWEPキーを選択することをお勧めします。ここでは、128bitキーの設定について解説します。

万が一WEPキーが破られることを想定して、定期的にWEPキーを変更することを推奨します。

設定ページ

■［詳細設定］→［PCカード設定］→［無線カード］

暗号化方式	WEP 128bit
オプション	card air11 wep key128 1 0h:1e:2d:3c:4b:5a:69:78:87:96:a5:b4:c3 card air11 wep default key 128 1 ※設定するのは、128bitのうち104bitです。 ※WEPキーは、0〜9、a〜hまでの16進数で入力します。 ※標準キーの初期値は「1」です。

◆［暗号化方式］を［WEP 64bit/128bit/152bit］を選択したときは、必ずWEPキーを設定してください。WEPキーを設定していないと、通信ができなくなります。また、設定したWEPキーは忘れないようにしてください。

◆本製品とパソコン側とで、同じWEPキーを設定してください。WEPキーが一致していないと通信ができなくなります。

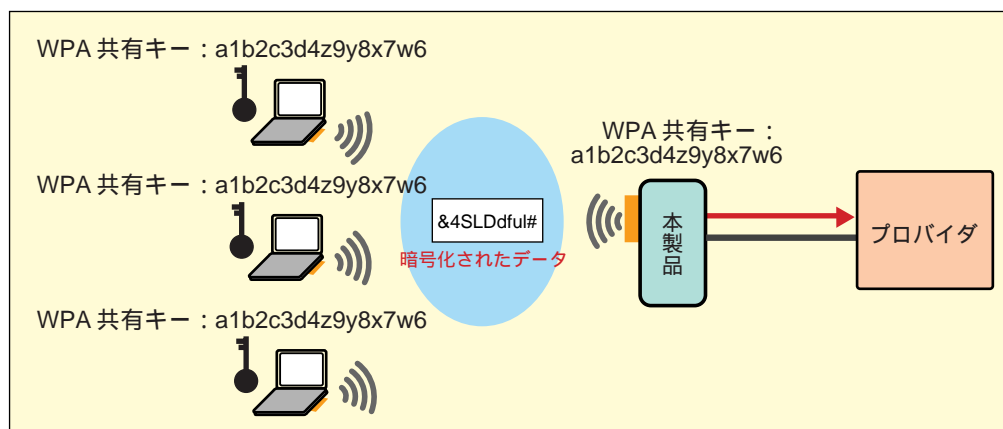
◆暗号化の設定をしたあと、無線LANで通信できなくなったとき

LANポートにつないでいるパソコンがある場合は、そのパソコンから本製品の設定ページを開き、［暗号化］を［しない］に変更してください。その後、もう一度暗号化の設定を行ってください。

すべてのパソコンを無線で接続しているときは、設定ページを開くことができません。本製品の設定を購入時の状態に戻してください。このとき、インターネットへの接続など、設定した内容がすべて消去されてしまいますので、ご了承ください。

無線LANの通信を暗号化する（WPA-PSKを使用する）

WPA-PSKを利用することで、無線LANのセキュリティを強化することができます。
お使いの無線LANカードもWPA-PSKに対応していることを確認してください。

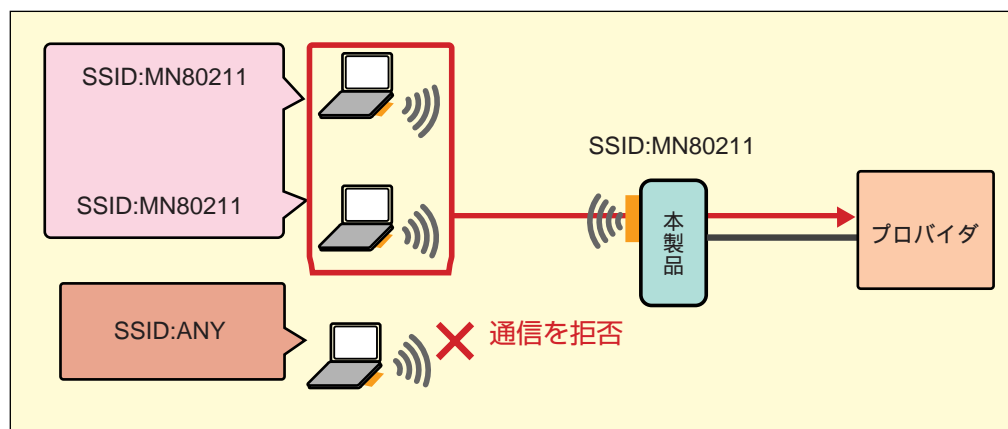
◆お使いの無線LANカードによっては、WPA-PSKを使用できるパソコンのOS が限定されている場合があります。
詳しくは無線LANカードに付属の取扱説明書をお読みください。

設定ページ

■［詳細設定］→［PCカード設定］→［無線カード］

認証	WPA-PSK
WPA 共有キー	a1b2c3d4z9y8x7w6 ※半角英数字 8 ～ 63 文字の範囲内で、任意の文字列を必ず入力してくだい。また、外部から推測されにくいものを設定してください。
暗号化方式	TKIP
鍵の変更更新間隔	1800 ※ 30 ～ 99999 の間で設定できます。 ※数値を小さくすると、鍵の更新が頻繁に行われるため、セキュリティは強固になりますが、スループットは低下します。 ※数値を小さくすると、鍵の更新間隔が空くため、セキュリティは弱くなりますが、スループットは向上します。 ※「0」を設定すると、暗号化の鍵は更新されなくなります。

◆本製品とパソコン側とで、同じWPA共有キーを設定してください。WPA共有キーが一致していないと通信ができなくなります。

SSIDが空白または「ANY」に設定された パソコンとの通信を拒否する

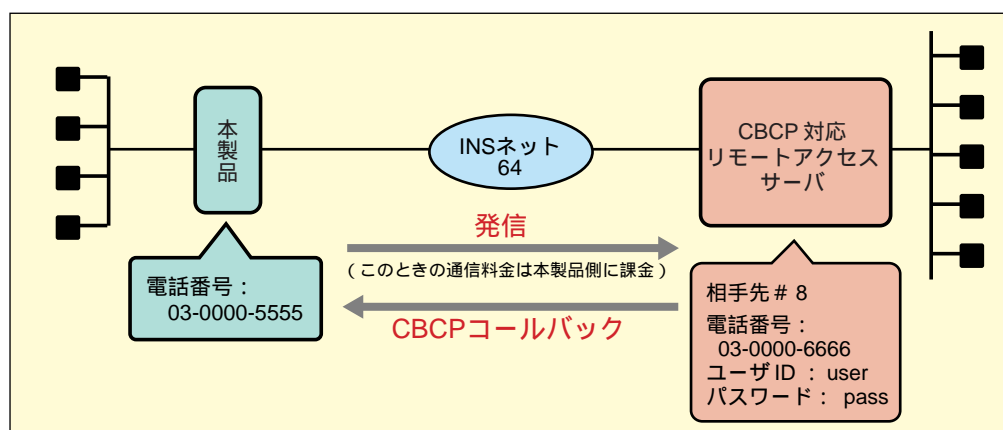
SSIDとは、無線LANで通信相手を特定するための識別記号のことです。本製品と本製品に接続するパソコンで同じSSIDを設定することで、無線LANで通信できるようになります。
無線LANの仕様では、パソコン側で「ANY」や空欄にしておくと、どのようなSSIDでも接続できます。本製品の「無線ステルス」機能を有効にすると、「ANY」や空白のSSIDでは本製品にアクセスできなくなります。また、Windows XPのワイヤレスネットワーク（Windows Zero Config）などから、設定しているSSIDを検索できなくなります。

設定ページ

■［詳細設定］→［PCカード設定］→［無線カード］

SSID	MN80211
無線ステルス	［有効］

無線ステルスを無効にしている場合は、設定しているSSIDは第三者が簡単に見ることができるので、SSIDにセキュリティとしての機能は期待できません。逆にSSIDに自分の名前や組織名など利用者を特定できる名前を設定すると、第三者に不要な興味を抱かせる可能性があります。出来るだけ意味を持たない名前を設定するようにしてください。

CBCPコールバック（ISDN、モデムカード）

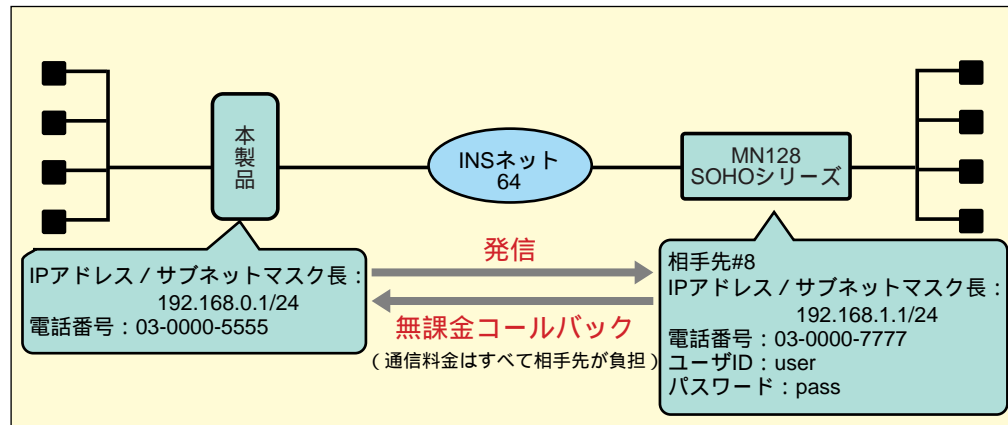
相手側のサーバがCBCP（Callback Control Protocol）に対応しているとき、コールバックさせることができます。なお、こちら（本製品）から接続するときの通信料金は、こちら（本製品）側に課金されます。

設定ページ

■ [詳細設定] → [接続／相手先登録] → [#8]

相手先名称	相手先の名称（何でも構いません）を設定
相手先電話番号	03-0000-6666
送信ユーザ ID	user
送信パスワード	pass
接続モード	［端末型接続］を選択
コールバック発信	［CBCP］を選択
折り返し電話番号	03-0000-5555 ※［ISDN 設定］画面の［ISDN 番号*サブアドレス］にかけ直してもらうときは、設定する必要ありません。

※上記以外の項目は、コールバック接続に関係ありません。

無課金コールバック

相手側の端末が本製品、MN128-SOHOシリーズ、MN128-Rのときには、こちら（本製品）から接続するときの通信料金を課金しない、「無課金コールバック」をすることができます。

設定ページ

■発信側（こちら側）で設定すること

● ［詳細設定］→［接続／相手先登録］→［#8］

相手先名称	相手先の名称（何でも構いません）を設定
相手先電話番号	03-0000-7777
送信ユーザ ID	user
送信パスワード	pass
接続モード	［端末型接続］を選択
コールバック発信	［無課金］を選択

● ［詳細設定］→［ルータ設定］→［LAN］

本体の IP アドレス／サブネットマスク長	192.168.0.1/24

● ［詳細設定］→［ルータ設定］→［ISDN］

ISDN番号*サブアドレス	03-0000-5555

無課金コールバックをしてもらうためには、発信側は相手先に発信電話番号を通知する必要があります。そのため、INSネット64の契約で「発信者番号通知サービス」を「通話ごと非通知（通常通知）」にしてください。

■受信側（相手側）で設定すること

● ［詳細設定］→［接続／相手先登録］→［#0］～［#15］のいずれか

相手先名称	こちら側の名称（何でも構いません）を設定
相手先電話番号	03-0000-5555
相手からの着信	［応じる］を選択
受信ユーザ ID	user
受信パスワード	pass
コールバック着信	［許可］または［コールバックのみ着信］を選択
折り返し電話番号	相手先が発信した電話番号と異なる電話番号にかけ直すときのみ、電話番号を設定します。通常は設定しません。

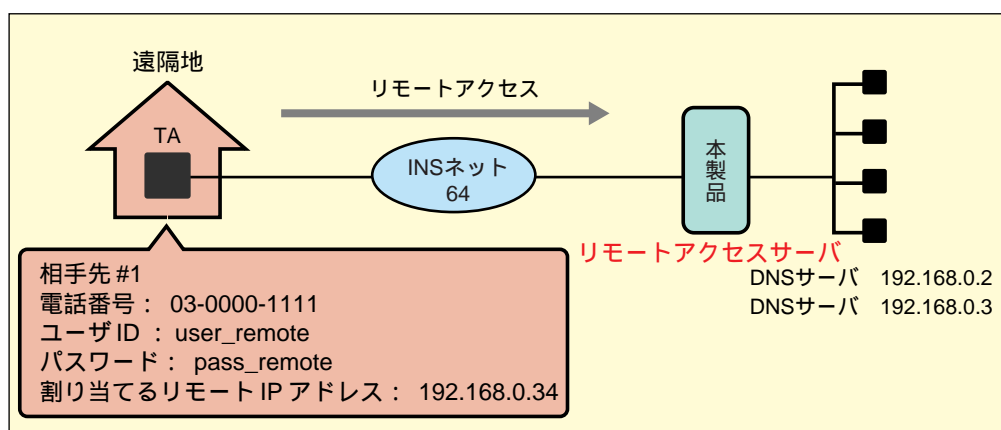
● ［詳細設定］→［ルータ設定］→［LAN］

本体の IP アドレス／サブネットマスク長	192.168.1.1/24
リモートアクセスサーバ機能	［ON］を選択
リモート IP アドレス	192.168.1.34 ※リモート IP アドレスは、4 つまで設定できます。 ※リモート IP アドレスを設定するときは、次のことに注意してください。 ・本製品と同じサブネットの IP アドレスを設定すること ・本製品の IP アドレス、LAN 上のほかのパソコンの IP アドレスおよび［USB ポート IP アドレス］で設定した IP アドレスのいずれとも重複しないように設定すること

● ［詳細設定］→［ルータ設定］→［ISDN］

ISDN番号*サブアドレス	03-0000-7777

リモートアクセスサーバにする

遠隔地のTAに接続されたパソコンから、本製品にリモートアクセスすることができます。本製品をリモートアクセスサーバにすると、同期64KbpsのHDLC（PPP）通信モード、128KbpsのMP通信モード、PIAFS通信モードで着信できます。

設定ページ

■ ［詳細設定］→［接続／相手先登録］→［#1］

相手先名称	相手先の名称（何でも構いません）を入力します。
相手先電話番号	03-0000-1111 ※空欄にすると、発信者の番号にかかわらず、着信を許可します。 ※相手先電話番号を設定した場合、リモートアクセスする側は発信者番号を通知する必要があります。
相手からの着信	［応じる］を選択
受信ユーザ ID	user_remote ※空欄にすると、着信時にユーザ ID による認証を行いません。
受信パスワード	pass_remote ※空欄にすると、着信時にパスワードによる認証を行いません。

※［相手先電話番号］を設定すると、設定した番号からの着信だけを許可します。
※［相手先電話番号］を空欄にした［接続／相手先登録］画面に該当した着信については、「該当する相手先の電話番号がないとき」〈P.98〉を参照してください。
※［受信ユーザID］［受信パスワード］を設定すると、相手先から着信した際、設定したユーザIDとパスワードを使って認証を行います。
※着信時の条件については、「着信してきた相手先の設定について」〈P.98〉を参照してください。

■ [詳細設定] → [ルータ設定] → [LAN]

本体の IP アドレス／サブネットマスク長	192.168.0.1/24
リモートアクセスサーバ機能	［ON］を選択
リモート IP アドレス	192.168.0.34 ※リモート IP アドレスは、4 つまで設定できます。 ※リモート IP アドレスを設定するときは、次のことに注意してください。 ・本製品と同じサブネットの IP アドレスを設定すること ・本製品の IP アドレス、LAN 上のほかのパソコンの IP アドレスで設定した IP アドレスのいずれとも重複しないように設定すること
AutoDNS 機能	［ON］を選択 ※ AutoDNS 機能を使用しない場合は、OFF にします。
LAN 側 DNS サーバアドレス（プライマリ）／LAN 側 DNS サーバアドレス（セカンダリ）	LAN 内にある DNS サーバを常に優先して使いたいときは、そのアドレスを設定します。 192.168.0.2 192.168.0.3 ※リモートアクセスするパソコンで、手動で DNS サーバを設定したいときは、この設定は不要です。

◆該当する相手先の電話番号がないとき

［接続／相手先登録］画面で相手先電話番号を指定しない場合、着信するときの認証プロトコルは［相手先に合わせる］に固定されてしまいます。［相手先名称］に「anonymous」と入力すると、PAPやCHAPなどの認証プロトコルを指定できます。

◆着信してきた相手先の設定について

本製品に着信すると、次の順に相手先からの情報と本製品の設定とを比較します。

（1）相手先電話番号の比較
相手先が通知した発信電話番号と一致する［接続／相手先登録］画面があるときは、以降、その内容に従います。相手先が発信電話番号を通知しないときや、一致する相手先の設定がないときは、［相手先電話番号］が空欄の［接続／相手先登録］画面の内容に従います。

（2）ユーザIDの比較
ユーザIDが一致する相手先があるときは、以降その内容に従います。一致する相手先の設定がないときは、［受信ユーザID］が空欄の［接続／相手先登録］画面の内容に従います。

パソコンの設定

■リモートアクセスするパソコン側の設定

リモートアクセスするパソコンのIPアドレスは、PPPサーバから取得するようにTCP/IPを設定します。

●Windows XPの場合

ダイヤルアップネットワークのリモートアクセスするためのアイコンの［インターネットプロトコル］で、［IPアドレスを自動的に取得する］を選択します。

●Windows 2000

［インターネットプロトコル］→［TCP/IPのプロトコル］で、［IPアドレスを自動的に取得］を選択します。

●Windows 98 SE/Me

ダイヤルアップネットワークのリモートアクセスするためのアイコンの［TCP/IP設定］で、［サーバーが割り当てたIPアドレス］を選択します。

●Macintosh

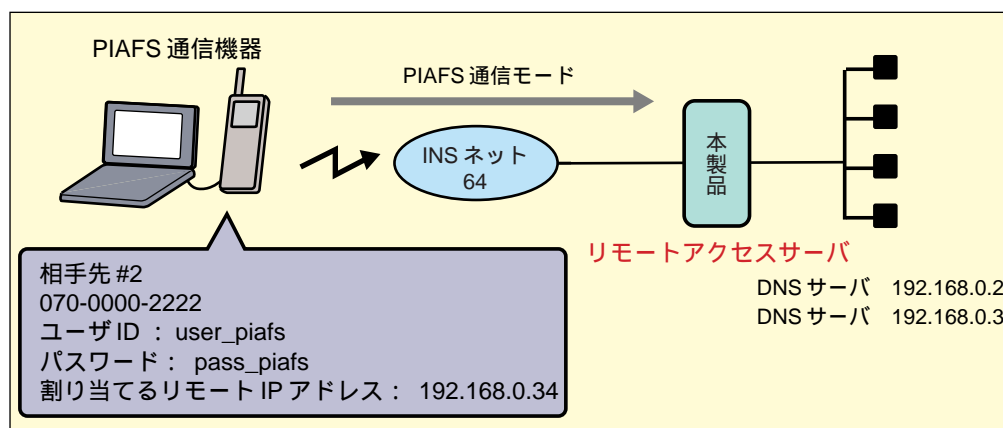
［認証方法］で［PPPサーバを参照］を選択します。

また、本製品でLAN内のDNSサーバのIPアドレスを設定していないときは、パソコンのTCP/IPでDNSサーバのIPアドレスを設定します。ただし、ドメイン名を使用しないときは必要ありません。

そのほかの設定については、リモートアクセスするパソコンが接続している通信機器の取扱説明書に従って操作してください。

PIAFS通信機器から着信する

本製品は、PHSとデータ通信を行うためのプロトコル「PIAFS」に対応しています。PIAFS通信可能な機器から着信することができます。

※NTT DoCoMoの方式やDDI POCKETの方式のPIAFS 64Kbpsに対応しています。

◆ コールバックの際の注意

PIAFS通信可能な機器で着信した際、こちら（本製品）側からコールバックすると、［情報表示（接続／切断ログ)］画面に通信料金が「0円」と表示されます。しかし、実際は接続時間に応じた通信料金がこちら（本製品）にかかりますので、ご注意ください。なお、本製品からのコールバックについて詳しくは、「コールバック着信する」〈P.103〉を参照してください。

設定ページ

■［詳細設定］→［接続／相手先登録］→［#2］

相手先名称	相手先の名称（何でも構いません）を入力します。
相手先電話番号	070-0000-2222 ※空欄にすると、発信者の番号にかかわらず、着信を許可します。 ※相手先電話番号を設定した場合、リモートアクセスする側は発信者番号を通知する必要があります。
相手からの着信	［応じる］を選択
受信ユーザ ID	user_piafs ※空欄にすると、着信時にユーザ ID による認証を行いません。
受信パスワード	passwd_piafs ※空欄にすると、着信時にパスワードによる認証を行いません。

※［相手先電話番号］を空欄にした［接続／相手先登録］画面に該当した着信については、「該当する相手先の電話番号がないとき」〈P.98〉を参照してください。

※［受信ユーザID］［受信パスワード］を設定すると、相手先から着信した際、設定したユーザIDとパスワードを使って認証を行います。

※着信の条件については「着信してきた相手先の設定について」〈P.98〉を参照してください。

■［詳細設定］→［ルータ設定］→［LAN］

本体のIPアドレス／サブネットマスク長	192.168.0.1/24
リモートアクセスサーバ機能	ONを選択
リモートIPアドレス1	192.168.0.34 ※リモートIPアドレスは、4つまで設定できます。 ※リモートIPアドレスを設定するときは、次のことに注意してください。 ・本製品と同じサブネットのIPアドレスを設定すること ・本製品のIPアドレス、LAN上のほかのパソコンのIPアドレスで設定したIPアドレスのいずれとも重複しないように設定すること
AutoDNS機能	ONを選択 ※AutoDNS機能を使用しない場合は、OFFにします。
LAN側DNSサーバアドレス（プライマリ）／LAN側DNSサーバアドレス（セカンダリ）	LAN内にあるDNSサーバを常に優先して使いたいときは、そのアドレスを設定します。 192.168.0.2 192.168.0.3 ※リモートアクセスするパソコンで手動でDNSサーバを設定したいときは、この設定は不要です。

パソコンの設定

■リモートアクセスするパソコン側の設定

リモートアクセスするパソコンのIPアドレスは、PPPサーバから取得するようにTCP/IPを設定します。

●Windows XPの場合

ダイヤルアップネットワークのリモートアクセスするためのアイコンの［インターネットプロトコル］で、［IPアドレスを自動的に取得する］を選択します。

●Windows 2000

［インターネットプロトコル］→［TCP/IPのプロトコル］で、［IPアドレスを自動的に取得］を選択します。

●Windows 98 SE/Me

ダイヤルアップネットワークのリモートアクセスするためのアイコンの［TCP/IP設定］で、［サーバーが割り当てたIPアドレス］を選択します。

●Macintosh

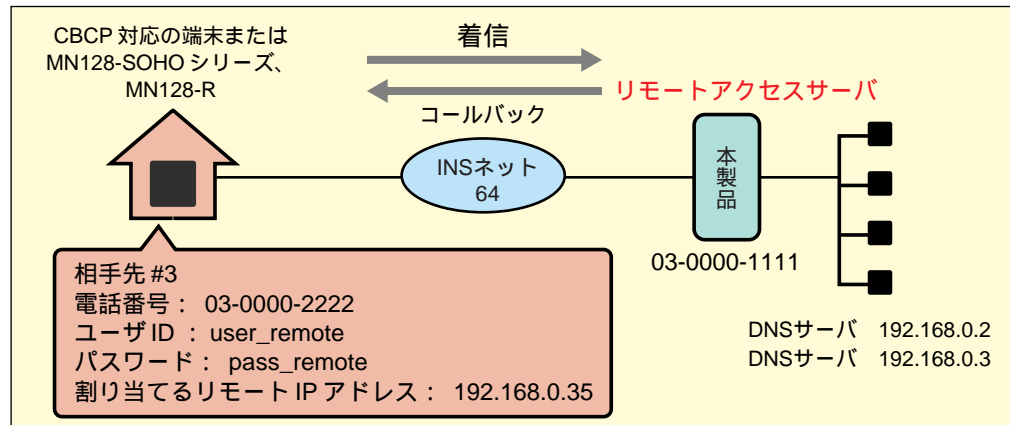
［認証方法］で［PPPサーバを参照］を選択します。

また、本製品でLAN内のDNSサーバのIPアドレスを設定していないときは、パソコンのTCP/IPでDNSサーバのIPアドレスを設定します。ただし、ドメイン名を使用しないときは必要ありません。

※PIAFS64Kbpsで通信するときは、番号を通知してください。設定方法はPHSやPIAFSカードのマニュアルを参照してください。

そのほかの設定については、アクセスするパソコンが接続している通信機器の取扱説明書に従ってください。

コールバック着信する

相手先からの着信を許可した際、こちら（本製品）から回線を接続し直してコールバックすることができます。また、相手先がコールバックを要求したときだけ、着信を許可することもできます。

通信料金は、こちら（本製品）側にかかります。ただし、コールバックを要求するはじめの接続時の通信料金は、相手先にかかります。
なお、コールバックできるのは、相手先がCBCP対応の端末（WindowsXP/2000/98 SE/Meのダイヤルアップネットワークなど）、もしくはMN128-SOHOシリーズ（本製品を含む）、MN128-Rを使っているときだけです。

PIAFS通信可能な機器で着信するときも、本製品からコールバックできます。その際、［情報表示（接続／切断ログ）］画面に通信料金が「0円」と表示されます。しかし、実際は接続時間に応じた通信料金がこちら（本製品）にかかりますので、ご注意ください。

設定ページ

■ [詳細設定] → [接続/相手先登録] → [#3]

相手先名称	相手先の名称（何でも構いません）を設定
相手先電話番号	03-0000-2222 ※空欄にすると、すべての番号からの着信を許可します。
相手からの着信	［応じる］を選択
受信ユーザ ID	user_remote ※空欄にすると、着信時にユーザ ID による認証を行いません。
受信パスワード	pass_remote ※空欄にすると、着信時にパスワード による認証を行いません。
コールバック着信	［許可］または［コールバックのみ着信］を選択
折り返し電話番号	03-0000-2222 ※相手先の端末が CBCP（Callback Control Protocol）に対応しているとき、あるいは、相手先が無課金コールバックを要求するときは、こちら（本製品）側からかけ直す電話番号を指定できます。 ※相手先が発信した電話番号にかけ直すとき、あるいは、相手先がかけ直す電話番号を指定するときは、設定しないでください。

※[相手先電話番号］を設定すると、設定した番号からの着信だけを許可します。
※[相手先電話番号］を空欄にした［接続／相手先登録］画面に該当した着信については、「該当する相手先の電話番号がないとき」〈P.98〉を参照してください。
※[受信ユーザID］［受信パスワード］を設定すると、相手先から着信した際、設定したユーザIDとパスワードを使って認証を行います。
※着信の条件については「着信してきた相手先の設定について」〈P.98〉を参照してください。

無課金コールバックの要求を許可するときは、相手先から発信電話番号を通知してもらう必要があります。

■［詳細設定］→［ルータ設定］→［LAN］

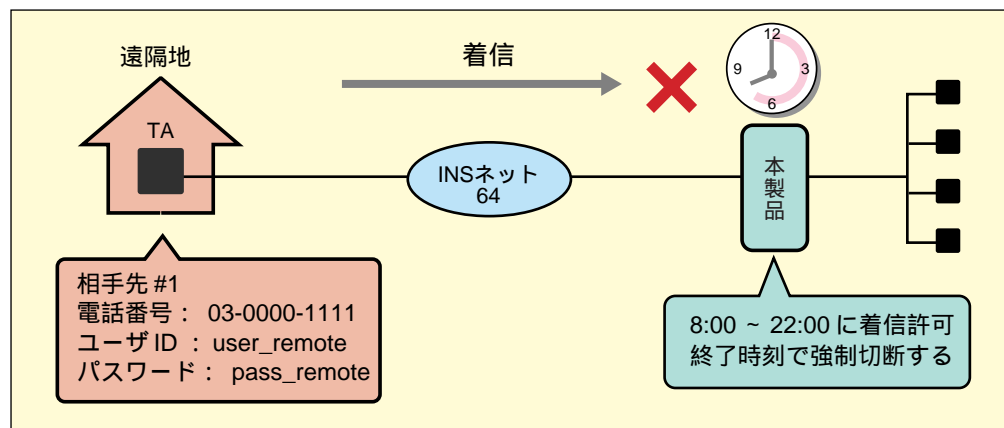
項目	設定
本体のIPアドレス／サブネットマスク長	192.168.0.1/24
リモートアクセスサーバ機能	［ON］を選択
リモートIPアドレス1	192.168.0.35 ※リモート IP アドレスは、4 つまで設定できます。 ※リモート IP アドレスを設定するときは、次のことに注意してください。 ・本製品と同じサブネットの IP アドレスを設定すること ・本製品の IP アドレス、LAN 上のほかのパソコンの IP アドレスのいずれとも重複しないように設定すること
AutoDNS機能	［ON］を選択 ※ AutoDNS 機能を使用しない場合は、OFF にします。
LAN側DNSサーバアドレス（プライマリ）／LAN側DNSサーバアドレス（セカンダリ）	LAN 内にある DNS サーバを常に優先して使いたいときは、そのアドレスを設定します。 192.168.0.2 192.168.0.3 ※リモートアクセスするパソコンで、手動で DNS サーバを設定したいときは、この設定は不要です。

◆本製品同士を接続する場合にコールバックするとき

本製品同士あるいはMN128-SOHOシリーズ、MN128-Rとの通信時にコールバック着信する場合、無課金コールバックできます。
ただし、コールバックを受ける側（こちら側）は、［接続／相手先登録］画面の［相手先電話番号］にコールバックを要求する側（相手先）電話番号を設定する必要があります。
また、コールバックを要求する側（相手先）は、「無課金コールバック」〈P.95〉を参照して設定を行ってください。

本製品同士でコールバックする場合、コールバックを受ける側（こちら側）は発信電話番号を通知してください。INSネット64の契約で、こちら側の「発信者番号通知サービス」を「通話ごと非通知」（通常通知）にしてください。

着信できる時間帯を制限する

着信できる時間帯を制限できます。

時間帯は、相手先ごとに開始時刻と終了時刻を指定して設定します。曜日の指定はできません。また、終了時刻になったとき、通信中でも強制的に自動切断するかどうか設定できます。

設定ページ

■ [詳細設定] → [接続／相手先登録] → [#1]

相手先名称	相手先の名称（何でも構いません）を設定
相手先電話番号	03-0000-1111
相手からの着信	［応じる］を選択
受信ユーザID	user_remote
受信パスワード	pass_remote
時間帯による着信制限	［以下の時間帯のみ着信許可］を選択
着信を許可する時間帯	08:00　時：分から　22:00 時：分まで
終了時刻で強制切断	［する］を選択

［終了時刻で強制切断］で［する］を選択した場合、通信中でも終了時刻になると自動切断します。

グローバル着信、サブアドレスグローバル着信を設定する

■グローバル着信について

グローバル着信とは、発信側からダイヤルした番号（着番号）の通知がない場合に、着信するかどうかを選択できる機能です。本製品では、着番号の通知がない着信を無視できます。着番号の通知があるかどうかは、INSネット64（ダイヤルイン）契約時の内容によります。それぞれの着信条件は次のようになります。

※下記の着信条件は、ルータ機能を使用するときの着信条件です。TELポートの着信条件は、リファレンスガイドブック「アナログ機器用ATコマンド・設定コードリファレンス」を参照してください。

●ダイヤルイン契約なしのとき

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">ISDN番号の設定（本製品）</td></tr>
<tr><td>なし</td><td>あり</td></tr>
<tr><td>着番号の通知</td><td>なし</td><td colspan="2">［グローバル着信］の設定が［する］のとき：着信
［グローバル着信］の設定が［しない］のとき：着信しない</td></tr>
</table>

●ダイヤルイン契約あり、グローバル着信を利用する契約のとき

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">ISDN番号の設定（本製品）</td></tr>
<tr><td>なし</td><td>あり</td></tr>
<tr><td rowspan="2">着番号の通知</td><td>なし
（契約者回線番号）</td><td colspan="2">［グローバル着信］の設定が［する］のとき：着信
［グローバル着信］の設定が［しない］のとき：着信しない</td></tr>
<tr><td>あり
（ダイヤルイン番号）</td><td>着信</td><td>番号が一致したときに着信</td></tr>
</table>

●ダイヤルイン契約あり、グローバル着信を利用しない契約のとき

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="2">ISDN番号の設定（本製品）</td></tr>
<tr><td>なし</td><td>あり</td></tr>
<tr><td>着番号の通知</td><td>あり
（契約者回線番号、ダイヤルイン番号）</td><td>着信</td><td>番号が一致したときに着信</td></tr>
</table>

■サブアドレスグローバル着信の設定をする

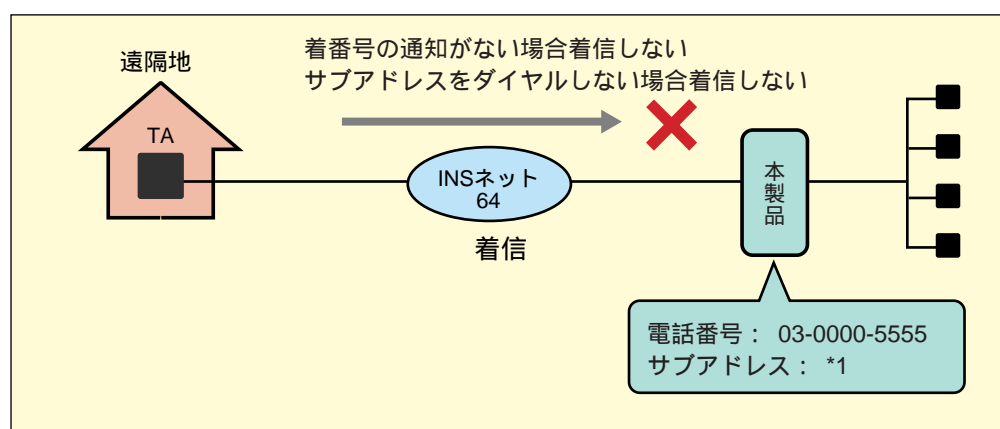
サブアドレスグローバル着信とは、発信側がサブアドレスをダイヤルしない場合、その着信を許可するかどうかを決める機能です。

本製品にサブアドレスを設定していると（自サブアドレス）、発信側がサブアドレスをダイヤルしなかった場合、その着信を無視することができます。自サブアドレスと発信側がダイヤルしたサブアドレス（着アドレス）の内容によって、それぞれの着信条件は次のようになります。

※下記の着信条件は、ルータ機能を使用するときの着信条件です。TELポートの着信条件は、リファレンスガイドブック「アナログ機器用ATコマンド・設定コードリファレンス」を参照してください。

		自サブアドレスの設定（本製品）	
		なし	あり
発信側 着サブアドレス	なし	着信	［サブアドレスグローバル着信］の設定が［する］のとき：着信 ［サブアドレスグローバル着信］の設定が［しない］のとき：着信しない
	あり	着信しない	サブアドレスが一致したときに着信

◆i・ナンバーを契約しているとき

i・ナンバーを契約しているときのグローバル着信の着信条件は、「ダイヤルイン契約なしのとき」〈P.107〉と同様です。サブアドレスグローバル着信の着信条件は、上記の表と同様です。

設定ページ

■［詳細設定］→［ルータ設定］→［ISDN］

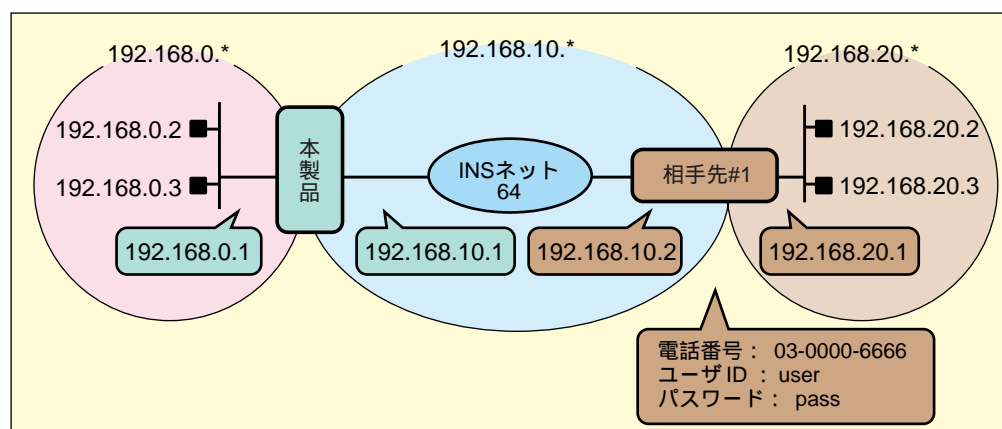
ISDN番号*サブアドレス	03-0000-5555*1
グローバル着信	しない
サブアドレス グローバル着信	しない

※着番号の通知がない着信を許可したいときは、［グローバル着信］で「する」を選択します。

※着サブアドレスがないときでも着信させたいときは、［サブアドレスグローバル着信］で「する」を選択します。

numbered接続する

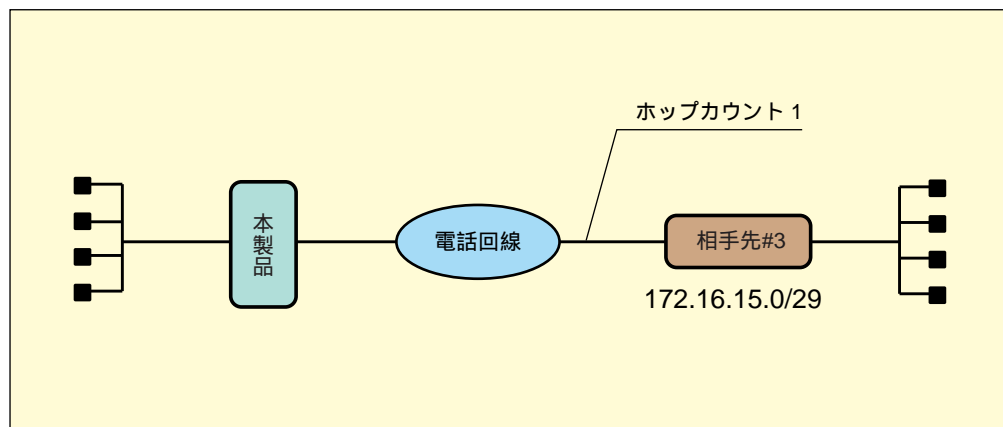
WAN回線側にネットワークを割り当てる接続です。
LAN型ダイヤルアップ接続する際に、相手先の使用しているルータがWAN回線側にネットワークを割り当てている場合は、本製品でもWAN回線側にネットワークを割り当てる必要があります。

※出荷時の本製品では、WAN回線側にネットワークを割り当てない「unnumbered接続」を行うように設定されています。

設定ページ

■ [詳細設定] → [接続／相手先登録] → [#8]

電話番号	03-0000-6666
送信ユーザ ID	user
送信パスワード	pass
接続モード	［LAN 型接続］を選択
オプション	remote 1 wanaddress 192.168.10.1/24

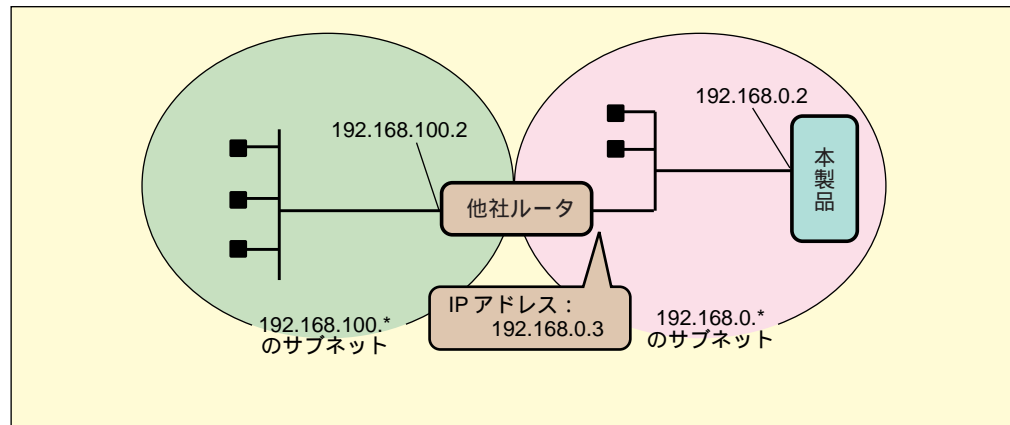
固定したルート（スタティックルート）で通信する（WAN側）

ネットワーク情報を流さない他社製のルータと本製品を接続するときなど、相手先のネットワーク情報を入手できない場合は、スタティックルートを設定します。

設定ページ

■ [詳細設定] → [ルータ設定] → [LAN]

オプション	ip route 172.16.15.0/29/1 remote 3 static

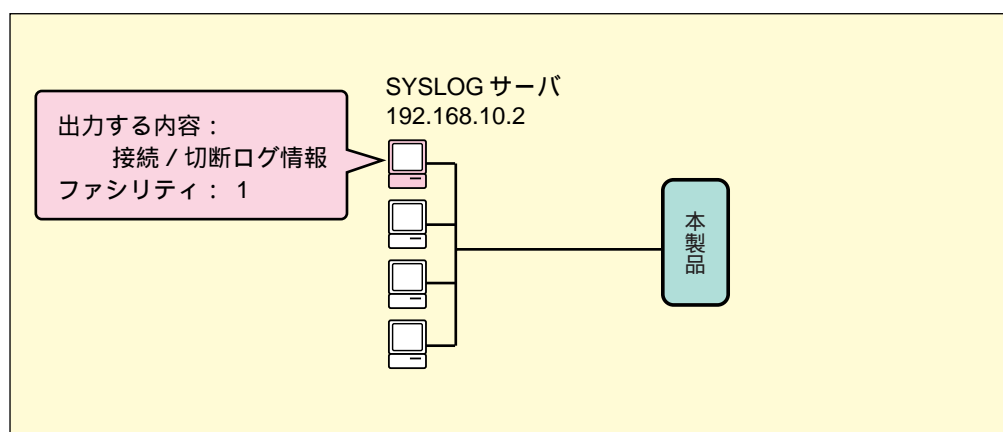
固定したルート（スタティックルート）で通信する（LAN側）

LAN側に、ネットワーク情報を流さない他社製のルータを接続する場合は、LAN側のスタティックルートを設定します。

設定ページ

■ [詳細設定] → [ルータ設定] → [LAN]

オプション	ip route 192.168.100.0/24/2 local 192.168.0.3

SYSLOGサーバに出力する

［情報表示（接続/切断ログ）］画面の記録やデバッグ情報（PPP接続に関する情報など）、フィルタリング情報（本製品に設定しているフィルタに該当したパケットの情報）や本製品で破棄されたパケット情報を、SYSLOGサーバに出力できます。ファイルとして一括管理できるので便利です。

※本製品にはSYSLOGサーバの機能はありません。SYSLOGサーバは別途用意してください。
また、SYSLOGサーバについては、それぞれの取扱説明書を参照してください。

設定ページ

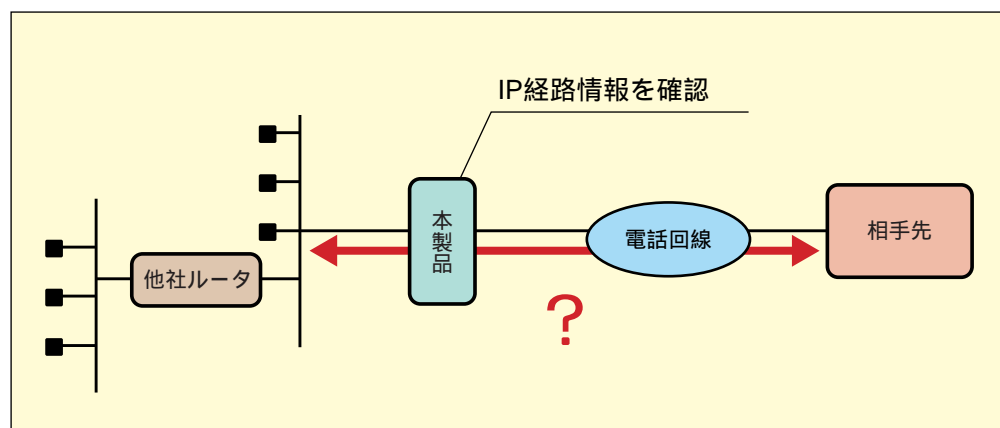
■ ［詳細設定］ → ［ルータ設定］ → ［LAN］

SYSLOG 機能	［INFO］をチェック
SYSLOG ホストアドレス	192.168.10.2
SYSLOG ファシリティ	1

［SYSLOG機能］で設定できる項目は次のとおりです。

DEBUG　：ISDNやPPPなど各種デバッグ情報を出力します。
INFO　：接続／切断ログ情報を出力します。
NOTICE　：パケットフィルタリングで処理されたすべてのパケットの内容、ステルスモードやSPI機能がONのとき破棄されたパケットのログを出力します。

IP経路情報を見る

本製品に登録されているIP経路の情報を確認できます。

設定ページ

■ [詳細設定] (またはクイック設定) → [情報表示] → [IP経路]

情報表示(IP経路) Help

◆現在のIP経路情報の一覧です。

```
# DNS Route

# Destination Route
    destination          gateway      mode  if   metric  ttl     remote
------------------ --------------- ---- ---- ------ ----- ----------
192.168.0.0/24     192.168.0.1     DRCT 0    0       -
192.168.0.1/32     192.168.0.1     DRCT 0    0       -
172.16.0.0/16      172.16.1.231    TERM 9    1       180
172.16.1.231/32    172.16.1.231    TERM 9    1       180
default            172.16.1.231    AUTO 9    1       180   #0
```

活用ガイド～中・上級編

付録

ここでは、おもに本製品を使用しているときのトラブル対処方法についてまとめています。困ったこと、わからないことがでてきたときにお読みください。

1 困ったときは

本製品が正常に動作しない場合は、該当する項目を確認してください。

ISDN、FOMA/PHS/モデムの対応PCカードのトラブル

■発着信できない

→［情報表示（接続／切断ログ)］画面を確認してください。履歴は表示されていますか？

エラーが表示されるときは、「設定ページのエラー一覧」〈P.133〉を参照して対処してください。エラーや履歴が表示されないときは、以下を参照して対処してください。

→［接続／相手先登録］画面の［相手先電話番号］が正しいか確認してください。

→［接続／相手先登録］画面の［送信ユーザID］が正しいか確認してください。

→［接続／相手先登録］画面の［送信パスワード］が正しいか確認してください。

→［接続／相手先登録］画面の［認証プロトコル］が正しいか確認してください。

→［接続／相手先登録］画面の［通信チャネル］が正しいか確認してください。

→発信は、３分間に３回だけ可能です。３分経過してから、もう一度発信してください。

→相手先に次のことを確認してください。

・ほかの通信機器が応答していませんか？
・各機器は正しく接続していますか？
・着信を許可していますか？

■コールバックで発信できない

→相手先にコールバックを許可しているか確認してください。

→［接続／相手先登録］画面の［コールバック発信］で［CBCP］を選択している場合、相手先の端末がCBCPに対応しているか確認してください。

→［接続／相手先登録］画面の［コールバック発信］で［無課金］を選択している場合、相手先がMN128-SOHOシリーズ（本製品含む）あるいはMN128-Rであるか確認してください。

■自動接続できない

→［自動接続相手先］画面で自動接続する相手を変更しませんでしたか？

自動接続したい相手先を選択してください。

→［接続／相手先登録］画面の［時間帯による制限］を「以下の時間帯のみ自動接続可能」に設定していると、［自動接続可能な時間帯］しか自動接続できません。

→［情報表示（自動接続制限)］画面を確認してください。［再接続制限］欄に「禁

止」と表示されている場合は、料金制限、回数制限、最大接続時間経過後の自動接続の制限のいずれかによって、自動接続を禁止されています。次のように対処してください。

- ［情報表示（自動接続制限）］画面で、自動接続を禁止している制限項目をリセットしてください。
- 料金制限、回数制限によって自動接続を禁止されている場合は、［接続相手先登録］画面の［料金による制限］（料金制限の場合）あるいは［接続回数による制限］（回数制限の場合）の数値を増やして、再設定してください。

→［情報表示（接続／切断ログ）］画面を確認してください。履歴は表示されていますか？

エラーが表示されるときは、「設定ページのエラー一覧」〈P.133〉を参照して対処してください。エラーや履歴が表示されないときは、以下を参照して対処してください。

→［ルータ設定（LAN）］画面の［オプション］に、自動接続のためのIP経路情報が正しく登録されているか確認してください。

→［情報表示（IP経路）］画面で自動接続先のルート（「mode」が「auto」と表示されているルート）が正しいか確認してください。

→［接続／相手先登録］画面から手動で相手先に接続できるか確認してください。

→［ルータ設定（LAN）］画面の［オプション］に登録されているフィルタ、IPアドレス変換テーブルやソース経路情報が正しいかどうか確認してください。

→ Windows XP/2000/98 SE/Meで自動接続できない場合は、次の原因が考えられます。

Windows XP/2000/98 SE/Me/を使用している場合、その仕様により、意図しない自動接続が発生してしまうことがあります。そのため、本製品では、購入時にあらかじめ次のフィルタが登録されています。

```
ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany
```

※フィルタ番号は、上記と異なる場合があります。

また、Windows 2000 Serverのドメインに所属するパソコンが、Microsoftネットワークにログオンする場合、Windows 2000 Serverと通信して、ログオン名とパスワードの認証を受けます。その際、Windows 2000 Serverが遠隔地にあるときは、上記のフィルタのために回線を自動接続することができません。
Microsoftネットワークにログオンするときや、共有フォルダへアクセスするときなどに、回線を自動接続したい場合は、［ルータ設定（LAN）］画面の［オプション］に登録されている上記のフィルタを削除してください。
ただし、これらのフィルタを削除すると、Windows XP/2000/98 SE/Meが遠隔地のワークグループまたはドメインに所属する場合、マスタブラウザへ定期的にアクセスするため、回線の自動接続が発生しますので、ご注意ください。

→ Windows 2000 Serverが自動接続できない場合は、次の原因が考えられます。

Windows 2000 Serverは、電源投入時にパソコンのIPアドレスをDNSサーバに登録する機能があります。そのため、本製品のAutoDNS機能を使用している場合に

は、パソコンの電源を入れると自動接続を行います。この自動接続を防ぐために、あらかじめ購入時の本製品には、次のフィルタが登録されています。

ip filter 60 reject dns qtype 6

※フィルタ番号は、上記と異なる場合があります。

LAN上のWindows 2000 ServerでIPアドレスをDNSサーバに登録したいときなどに、回線を自動接続したい場合は、[ルータ設定（LAN）] 画面の［オプション］に記載されている上記のフィルタを削除してください。
ただし、上記のフィルタを削除すると、LAN上にWindows 2000 Serverがある場合、自動接続が発生します。ご注意ください。

■勝手に接続してしまう

→ LAN上にWindows XP/2000/98 SE/Me/があるとき、意図しない自動接続が行われていることがあります。

通常、Windows XP/2000/98 SE/Meを接続しているルータを自動接続するように設定すると、意図的に通信操作を行わなくても、定期的に（約15秒ごと）自動接続してしまいます。これは、Windows XP/2000/98 SE/Meの仕様のために発生します。この自動接続を防ぐために、あらかじめ本製品には、購入時の設定で次のフィルタが登録されています。

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

※フィルタ番号は、上記と異なる場合があります。

・ip filter 61
パソコン上でWWWブラウザを終了するときに送信される、不要なパケットによる自動接続を防止するためのフィルタです。なお、「tcpfin」はTCPのセッションによる終了時のTCPパケットだけを対象にします。

・ip filter 64
指定のポートを使用する、自動接続のきっかけとなるパケット（トリガパケット）を破棄するためのフィルタです。なお、手動で接続したときや、すでに回線が接続されているときは、指定のポートを使用して通信を行うことができます。
フィルタは、［ルータ設定（LAN）］画面の［オプション］で確認・削除することができます。
ただし、次のケースに当てはまる場合は、Windows XP/2000/98 SE/Meで設定を行う必要があります。

▼ケース1
WindowsのTCP/IPの設定で、相手先のDNSサーバアドレスを指定している、または、AutoDNS機能を使用し本製品にLAN側のDNSサーバアドレスを指定していない場合
●Windows XP/2000
［インターネットプロトコル（TCP/IP）のプロパティ］を開きます。［詳細設定］ボタンをクリックして［TCP/IP詳細設定］ダイアログを開き、次のように設定します。

・［DNS］タブで［この接続のアドレスをDNSに登録する］のチェックを外す
・［WINS］タブで［NetBIOS over TCP/IPを無効にする］を選択

●Windows 98 SE/Me
特別な設定は必要ありません。

▼ケース2
WindowsのTCP/IPの設定でLAN側のDNSサーバアドレスを指定している、または、AutoDNS機能を使用し、本製品にLAN側のDNSサーバアドレスを設定している場合

●Windows XP/2000
［インターネットプロトコル（TCP/IP）のプロパティ］を開きます。［詳細設定］ボタンをクリックして［TCP/IP詳細設定］ダイアログを開き、次のように設定します。
・［DNS］タブで［この接続のアドレスをDNSに登録する］のチェックを外す
・［WINS］タブで［NetBIOS over TCP/IPを無効にする］を選択

●Windows 98 SE/Me
DNSサーバを使用しないように設定します。
しかし、Windows98 SE/Meは、ホスト名やワークグループ名の問い合わせを解決するために、必ずDNSサーバを使用する仕様になっています。そのため、コントロールパネルで設定を変更することができません。
したがって、DNSサーバを使用しないように設定するには、レジストリと呼ばれるシステムのデータベースを直接書き換えてください。レジストリの書き換え方法は、マイクロソフト社の「Knowledge Base」と呼ばれるサポート用データベースに記載されているので（Article ID:Q137368）、米マイクロソフト社のホームページなどから参照できます。
なお、レジストリに関する操作は、システムクラッシュなどの危険が伴いますので、十分注意しながら行ってください。詳しくは、パソコンのマニュアルなどを参照してください。

▼その他
ほかにも、意図しない自動接続が行われてしまうことがあります。その場合は、自動接続のきっかけとなったパケット（トリガパケット）を確認し、送信元のパソコンの設定を見直してください。または、そのトリガパケットを破棄し、意図しない自動接続が行われないようにするためのフィルタを設定してください。

●自動接続の原因となる通信を行っているパソコンを限定する
1. ［情報表示（接続／切断ログ）］画面を開きます。
2. 「ルータ発信」という項目で、「トリガパケット」という文字が入っているログを探します。

```
ルータ（自動発信）［B1］：番号［0300001234］トリガパケット［UDP 192.168.0.3/ntp
-->172.16.0.129/ntp
```

この例では、「192.168.0.3のパソコンが、172.16.0.129のパソコンにUDP（ntp）の通信を行おうとして自動接続が起きた」ということを表しています。
この場合、192.168.0.3のパソコンの設定を確認してください。

●限定されたパソコンが自動接続を行わないようにフィルタを設定する
1. ［ルータ設定（LAN）］画面を開きます。

2. ［オプション］欄で、フィルタを設定します。

```
ip filter 1 restrict out 192.168.0.3 * udp ntp ntp remote *
```

この例は、192.168.0.3のパソコンが、172.16.0.129のパソコンにUDP（ntp）の通信を行おうとして自動接続が起きている場合に設定するフィルタです。
※フィルタについて詳しくは、「IPフィルタの設定」〈P.83〉を参照してください。

ケース1、ケース2の場合、Microsoftネットワークを使用して相手先のWindows XP/2000/98 SE/Me/の共有フォルダを利用できなくなります。これは、購入時のフィルタや上記の設定によって、ホストのIPアドレスの問い合わせを解決できなくなるためです。
この場合は、「Windows間で共有フォルダを利用する」〈P.75〉に従って設定してください。本製品を簡易DNSサーバとして使うときに、LAN上のパソコンのホスト名を登録しておくと、そのパソコンへアクセスする際、相手先に自動接続してしまうことはありません。「簡易DNSサーバにする」〈P.22〉を参照してください。

→ LAN上にWindows 2000があるとき、意図しない自動接続が行われてしまうことがあります。この自動接続を防ぐために、Windows 2000側または本製品側で設定をする必要があります。

▼Windows 2000側で設定するとき

1. ［コントロールパネル］→［ネットワークとダイヤルアップ接続］を開き、［ローカルエリア接続］を右クリックしてプロパティを開きます。
［ローカルエリア接続のプロパティ］ウィンドウが開きます。
2. ［インターネットプロトコル（TCP/IP)］をリストから選択し、［プロパティ］ボタンをクリックします。
［インターネットプロトコル（TCP/IP）のプロパティ］ウィンドウが開きます。
3. ［詳細設定］ボタンをクリックします。
［TCP/IP詳細設定］ウィンドウが開きます。
4. ［DNS］タブの［DNSドメイン名］の下に［この接続のアドレスをDNSに登録する］のチェックを外します。
5. ［OK］ボタンをクリックします。
手順2～4で開いたウィンドウをすべて閉じます。

▼本製品側で設定するとき

1. ［ルータ設定（LAN)］画面を開きます。
2. ［AutoDNS機能］をONにします。
3. DNS Queryパケットに関するIPフィルタを登録します。
   ip filter N reject dns qtype 6
   ※Nには1～64までの数字を入力します。
   ※クィック設定を行うと、「ip filter 60 reject dns qtype 6」が設定されます。
   ※すべての設定を消去すると、自動的にこのフィルタが登録されます。
4. ホスト情報にローカルエリア接続のドメイン名を登録します。
   ip host xxx.xxx.xxx.xxx ###
   ※「xxx.xxx.xxx.xxx」には、LAN内で使用していないIPアドレスを、「###」には、Windows2000に設定しているドメインまたはワークグループを入力してください。
   ドメインやワークグループは、［マイコンピュータ］→［ネットワークID］タブの

［詳細設定］で確認できます。

5.［設定］ボタンをクリックします。

ネットワークの設定内容や運用によっては、長時間、回線が接続したままになることや意図していない自動接続が行われていることがあります。初期導入後は、必ず［切断／接続状況］画面、［情報表示（通信料金）］画面を確認してください。

■着信できない

→［情報表示（接続／切断ログ）］画面でログを見て、ログが残っていれば何が原因かを確認してください。

→［接続／相手先登録］画面の［相手からの着信］を［応じる］に設定しているか確認してください。

→［接続／相手先登録］画面の［相手先電話番号］が正しいか確認してください。

→［接続／相手先登録］画面の［受信ユーザID］が正しいか確認してください。

→［接続／相手先登録］画面の［受信パスワード］が正しいか確認してください。

→［接続／相手先登録］画面の［認証プロトコル］（［受信パスワード］の下）が正しいか確認してください。

→［接続／相手先登録］画面の［時間帯による着信制限］を［以下の時間帯のみ着信許可］に設定していると、［着信を許可する時間帯］しか着信できません。

→ 相手先がTAの場合、次のことを確認してください。

- ［ルータ設定（LAN）］画面の［リモートアクセスサーバ機能］をONにしていますか？
- ［ルータ設定（LAN）］画面の［リモートIPアドレス1/2/3/4］に相手先に割り当てるIPアドレスを正しく設定していますか？

→ ほかの通信機器が応答していないか確認してください。

ISDN回線に複数の通信端末が接続されている場合、各端末にサブアドレスを設定してください。サブアドレスを設定すると、各端末を区別して着信できます。

■相手先と通信できない

→ パソコンのTCP/IPの設定が正しいか確認してください。

- パソコンのIPアドレスとサブネットマスクを正しく設定していますか？
- ゲートウェイを正しく設定していますか？
- DNSサーバのIPアドレスを正しく設定していますか？

→ 端末型ダイヤルアップ接続する場合、［切断／接続状況］画面の［割り当てIPアドレス］でIPアドレスを取得しているか確認してください。

→ フィルタ（［ルータ設定（LAN）］画面の［オプション］で設定）を正しく登録しているか確認してください。

→ 相手先によっては、AutoDNS機能が正常に働かないことがあります。

接続する相手先が設定されている［接続／相手先登録］画面の［DNSサーバアドレス］に、相手先のDNSサーバのIPアドレスを入力してください。

→ ご使用の通信ソフトの設定を確認してください。

プロキシサーバを正しく指定していますか？

→ 相手先が他社のルータを使用している場合、スタティックルートの設定が必要なことがあります。「固定したルート（スタティックルート）で通信する（WAN側）」〈P.110〉を参照してください。

→ LAN型ダイヤルアップ接続する場合、次のことを確認してください。

- こちら側のLANと相手先のLANに、異なるサブネットワーク番号を使用してください。
- numbered接続のときは、WAN側のIPアドレスの設定が必要です。→「numbered接続する」〈P.109〉を参照
- numbered接続するときは、WAN側のサブネットマスクの設定が必要なことがあります。→「numbered接続する」〈P.109〉を参照

■データ通信中に回線が切断されてしまう

→［情報表示（接続／切断ログ）］画面でどちら側から切断したのかを確認してください。

「こちらから切断」と表示されているときは、以下を参照して対処してください。
「相手先から切断」と表示されているときは、相手先に問い合わせてください。

→［接続／相手先登録］画面の［自動切断タイマ１］を設定していると、設定した時間、回線上で通信がなかったときは自動的に回線が切断されます。自動切断を止めたいときは、［自動切断タイマ１］に「0」を設定してください。

この場合、接続したら必ず手動で切断してください。

特に次の環境で本製品を使用しないように注意してください。

- すでに稼動しているLANに本製品を導入する際、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行う設定にしているとき
- LAN上のパソコンで定期的に回線を接続して通信を行うソフトウェアを起動しているとき

※［切断／接続状況］画面や［情報表示（通信料金）］画面で、回線の使用状況や通信料金を確認してください。

→［接続／相手先登録］画面の［使用するタイマ］を「タイマ1、以下の時間帯のみタイマ2に変更」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［タイマ２の時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

→［接続／相手先登録］画面の［最大接続時間］を設定していないか確認してください。

→［接続／相手先登録］画面の［時間帯による制限］を「以下の時間帯のみ自動接続可能」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［自動接続可能な時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

→［接続／相手先登録］画面の［時間帯による着信制限］を「以下の時間帯のみ着信許可」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［着信を許可する時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

■自動切断しない

→［接続／相手先登録］画面の［自動切断タイマ1］を「0」に設定していると自動切断しません。

→［接続／相手先登録］画面の［使用するタイマ］を「タイマ1、以下の時間帯のみタイマ2に変更」、かつ、［自動切断タイマ2］を「0」に設定していると、［タイマ２の時間帯］は自動切断しません。

→ 相手先と通信が行われていないか確認してください。

→ LAN上のすべての機器の電源をOFFにする、あるいは、LAN上の各機器のケーブルをすべて外してみてください。自動切断する場合は、LAN上の機器が相手先と通信している可能性があります。LAN上の各機器の設定を確認してください。

すべての機器を外しても切断しないときは、相手からパケットが送信されている可能性があります。その場合は、自動切断せずに必ず手動で切断してください。

→ 本製品が受信したパケットによって、［自動切断タイマ1/2］がリセットされ、自動切断ができなくなることがあります。

なお、次のパケットの場合は、リセットされません。

（1）Echo 、EchoReply以外のICMPパケット
ICMPパケットではリセットされません。ただし、pingではリセットされます。

（2）ブロードキャストUDPパケット
Destinationアドレスがすべて1、またはホスト部がすべて1のパケットではリセットされません。

（3）以下のサービスのUDPポート
Destinationポートが以下のパケットではリセットされません。
RIP（520）、NTP（123）、RWHO（513）、AT_ZIS（206）、ATLS（216）、SUNRPC（111）、 BOOTPC（68）、BOOTPS（67）、KIP（200..205）

（4）DNAME検索のUDPパケット
Sourceポート番号、またはDestinationポート番号がDNAME（53）のパケットでは、リセットされません。

（5）PPTP（1723）のTCPパケット
PPTPパケットではリセットされません。

（6）GRE（プロトコル番号47）のKeepAliveパケット
PPTP接続後GREプロトコルによって行われるKeepAliveパケットではリセットされません。
また、GREパケット内に含まれるIPパケットの内容が（1）～（4）に該当する場合は、リセットされません。

■本製品同士で接続できない

→ 発信側の場合、［ルータ設定（ISDN）］画面の［ISDN番号*サブアドレス］に、相手先に通知する電話番号（自分側の電話番号）を設定してください。本製品を購入時の設定のまま使用していると、［ISDN番号*サブアドレス］にはサブアドレス「1」が設定されているため、相手先にサブアドレス付きの番号が通知され、着信できないことがあります。

→ 着信側の場合、[情報表示（接続／切断ログ）] 画面で相手に通知された電話番号を確認し、それと同じ電話番号を［接続／相手先登録］画面の［相手先電話番号］に設定してください。

■FTPソフトでファイルの送受信ができない

→次のように、FTPソフトの設定を「PASVモード」に変更してください。

・Windows用　NextFTP（Ver.1.91）の場合
［オプション］→［ファイヤーウォール（プロキシ）］タブで［PASVモード］をチェックします。

・Macintosh用　Fetch（Ver.3.0.3J2）の場合
［初期設定］→［Firewall］で［パッシブモード転送（PASV）を使う］をチェックします。

※FTPによるデータ転送は、通常、サーバ側からクライアント側へアクセスした後にデータ転送を開始する仕組みになっています。しかし、本製品の購入時の設定では、外部からの不正なアクセスを防止するため、WAN側から本製品へのアクセスができないようになっています。そのため、FTPサーバからクライアント側へのアクセスもできません。「PASVモード」とは、この現象を回避するため、クライアント側からサーバ側へアクセスするようにした転送方法です。

■Windows Messenger / MSN Messengerで通信ができない

→ 本製品とWindows XP/MeのUPnPの設定を確認してください。Messengerを利用するときは、本製品とWindows XP/MeともにUPnP機能をONする必要があります。

●本製品のUPnP設定をONにする

1. ［詳細設定］→［UPnP設定］をクリックし、［UPnP機能］を［ON］にします。

●Windows XPのUPnP設定をONにする

1. ［スタート］メニューの［コントロールパネル］をクリックし、［ネットワーク接続］をクリックします。
   ［ネットワーク接続］ウィンドウが表示されます。
2. ［詳細設定］メニューから［オプションネットワークコンポーネント］を選択します。
3. コンポーネントの一覧で［ネットワークサービス］をクリックし、［詳細］ボタンをクリックします。
4. ［ネットワークサービス］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。
   チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows XPの画面の指示に従ってください。

●Windows MeのUPnP設定をONにする

1. ［スタート］メニューの［設定］から、［コントロールパネル］をクリックします。
2. ［アプリケーションの追加と削除］アイコンをダブルクリックして、［Windowsファイル］タブをクリックします。

3. ［コンポーネントの種類］で［通信］をクリックし、［詳細］ボタンをクリックします。
4. ［コンポーネントの種類］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。
   チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows Meの画面の指示に従ってください。

→ 通信相手の動作環境を確認してください。通信相手がUPnP対応のルータを使用していますか？または、プライベートIPアドレスを使用しているプロバイダ経由で接続していませんか？このような場合は、Messengerで通信できません。

→ Messengerでの通信がなくなってから、本製品のUPnPポート自動削除設定で設定した時間が経過したときは、自動的に使用されていたポートが閉じます。ポートが閉じてから再びMessengerを使いたいときは、Messengerをいったん終了してから、起動し直してください。Messengerでサインインし直すだけでは正常に動作しませんのでご注意ください。

ブロードバンドのトラブル

■ブロードバンド接続ができない

→「情報表示（接続/切断ログ）」画面を確認してください。履歴は表示されていますか？

エラーが表示されるときは、「設定ページのエラー一覧」〈P.133〉を参照して対処してください。エラーや履歴が表示されないときは、以下を参照して対処してください。

→「接続／相手先登録」画面の「送信ユーザID」が正しいか確認してください。

→「接続／相手先登録」画面の「送信パスワード」が正しいか確認してください。

→「接続／相手先登録」画面の「認証プロトコル」が正しいか確認してください。

→「接続／相手先登録」画面の「暗号化」が正しいか確認してください。

→ ブロードバンド接続には、「PPPoE（端末型）」「PPPoE（LAN型）」「DHCP」「Static」の異なる設定方法があります。プロバイダの契約（接続形態）と設定している画面が一致していますか？

→ 本製品前面のWANのランプを確認してください。

点灯していない場合は、ケーブルが外れているか、ケーブルが切断されている場合があります。

→ PPPoEランプを確認してください。

クイック設定でPPPoEを設定した場合、もしくは 詳細設定で通信チャネルを「PPPoE（ランプ点灯）」で設定した場合は、PPPoEランプが点灯します。点灯しない場合は「送信ユーザID」「送信パスワード」などの設定を再確認してください

→ プロバイダの工事は終了していますか？

契約を申し込んでから、工事が完了するまで日数がかかる場合があります。申し込んだプロバイダに確認してください。

→ クイック設定をしたあと、別のクイック設定をしませんでしたか？

「クイック設定」ページの［PPPoE（端末型）］、［PPPoE（LAN型）［端末型ダイヤルアップ］［フレッツ・ISDN］の各画面は、詳細設定ページの「接続/相手先登録」画面の各相手先番号と共通です。1つの画面で設定を変更すると、他の画面の設定も同じように変更されます。

■ブロードバンド回線で再接続できない

→ ケーブルを抜いたり、正常に切断処理をしないで本装置の電源を切った場合にはしばらく（数分間）再接続できないことがあります。しばらくたってから再接続してみてください。

■自動接続できない

→［自動接続相手先］画面で自動接続する相手を変更しませんでしたか？

自動接続したい相手先を選択してください。

→［接続／相手先登録］画面の［時間帯による制限］を「以下の時間帯のみ自動接続可能」に設定していると、［自動接続可能な時間帯］しか自動接続できません。

→［情報表示（自動接続制限）］画面を確認してください。［再接続制限］欄に「禁止」と表示されている場合は、料金制限、回数制限、最大接続時間経過後の自動接続の制限のいずれかによって、自動接続を禁止されています。次のように対処してください。

- ［情報表示（自動接続制限）］画面で、自動接続を禁止している制限項目をリセットしてください。
- 料金制限、回数制限によって自動接続を禁止されている場合は、［接続相手先登録］画面の［料金による制限］（料金制限の場合）あるいは［接続回数による制限］（回数制限の場合）の数値を増やして、再設定してください。

→［情報表示（接続／切断ログ）］画面を確認してください。履歴は表示されていますか？

エラーが表示されるときは、「設定ページのエラー一覧」〈P.133〉を参照して対処してください。エラーや履歴が表示されないときは、以下を参照して対処してください。

→［ルータ設定（LAN）］画面の［オプション］に、自動接続のためのIP経路情報が正しく登録されているか確認してください。

→［情報表示（IP経路）］画面で自動接続先のルート（「mode」が「auto」と表示されているルート）が正しいか確認してください。

→［接続／相手先登録］画面から手動で相手先に接続できるか確認してください。

→［ルータ設定（LAN）］画面の［オプション］に登録されているフィルタ、IPアドレス変換テーブルやソース経路情報が正しいかどうか確認してください。

→ Windows XP/2000/98 SE/Meで自動接続できない場合は、次の原因が考えられます。

Windows XP/2000/98 SE/Me/を使用している場合、その仕様により、意図しない自動接続が発生してしまうことがあります。そのため、本製品では、購入時にあらかじめ次のフィルタが登録されています。

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

※フィルタ番号は、上記と異なる場合があります。

また、Windows 2000 Serverのドメインに所属するパソコンが、Microsoftネットワークにログオンする場合、Windows2000 Serverと通信して、ログオン名とパスワードの認証を受けます。その際、Windows2000 Serverが遠隔地にあるときは、上記のフィルタのために回線を自動接続することができません。
Microsoftネットワークにログオンするときや、共有フォルダへアクセスするときなどに、回線を自動接続したい場合は、［ルータ設定（LAN）］画面の［オプション］に登録されている上記のフィルタを削除してください。
ただし、これらのフィルタを削除すると、Windows XP/2000/98 SE/Meが遠隔地のワークグループまたはドメインに所属する場合、マスタブラウザへ定期的にアクセスするため、回線の自動接続が発生しますので、ご注意ください。

→ Windows 2000 Serverが自動接続できない場合は、次の原因が考えられます。

Windows 2000 Serverは、電源投入時にパソコンのIPアドレスをDNSサーバに登録する機能があります。そのため、本製品のAutoDNS機能を使用している場合には、パソコンの電源を入れると自動接続を行います。この自動接続を防ぐために、あらかじめ購入時の本製品には、次のフィルタが登録されています。

ip filter 60 reject dns qtype 6

※フィルタ番号は、上記と異なる場合があります。

LAN上のWindows 2000 ServerでIPアドレスをDNSサーバに登録したいときなどに、回線を自動接続したい場合は、［ルータ設定（LAN）］画面の［オプション］に記載されている上記のフィルタを削除してください。
ただし、上記のフィルタを削除すると、LAN上にWindows 2000 Serverがある場合、自動接続が発生します。ご注意ください。

■相手先と通信できない

→ パソコンのTCP/IPの設定が正しいか確認してください。

- パソコンのIPアドレスとサブネットマスクを正しく設定していますか？
- ゲートウェイを正しく設定していますか？
- DNSサーバのIPアドレスを正しく設定していますか？

→ 端末型ダイヤルアップ接続する場合、［切断／接続状況］画面の［割り当てIPアドレス］でIPアドレスを取得しているか確認してください。

→ フィルタ（［ルータ設定（LAN）］画面の［オプション］で設定）を正しく登録しているか確認してください。

→ 相手先によっては、AutoDNS機能が正常に働かないことがあります。

接続する相手先が設定されている［接続／相手先登録］画面の［DNSサーバアドレス］に、相手先のDNSサーバのIPアドレスを入力してください。

→ ご使用の通信ソフトの設定を確認してください。

プロキシサーバを正しく指定していますか？

→ 相手先が他社のルータを使用している場合、スタティックルートの設定が必要なことがあります。「固定したルート（スタティックルート）で通信する（WAN側）」〈P.110〉を参照してください。

→ LAN型ダイヤルアップ接続する場合、次のことを確認してください。

- こちら側のLANと相手先のLANに、異なるサブネットワーク番号を使用してください。
- numbered接続のときは、WAN側のIPアドレスの設定が必要です。→「numbered接続する」〈P.109〉を参照
- numbered接続するときは、WAN側のサブネットマスクの設定が必要なことがあります。→「numbered接続する」〈P.109〉を参照

■データ通信中に回線が切断されてしまう

→ ［情報表示（接続／切断ログ）］画面でどちら側から切断したのかを確認してください。

「こちらから切断」と表示されているときは、以下を参照して対処してください。
「相手先から切断」と表示されているときは、相手先に問い合わせてください。

→ ［接続／相手先登録］画面の［自動切断タイマ１］を設定していると、設定した時間、回線上で通信がなかったときは自動的に回線が切断されます。自動切断を止めたいときは、［自動切断タイマ１］に「0」を設定してください。

この場合、接続したら必ず手動で切断してください。

特に次の環境で本製品を使用しないように注意してください。

- すでに稼動しているLANに本製品を導入する際、本製品にLANと同じサブネットのIPアドレスを設定しないまま、自動接続を行う設定にしているとき
- LAN上のパソコンで定期的に回線を接続して通信を行うソフトウェアを起動しているとき

※［切断／接続状況］画面や［情報表示（通信料金）］画面で、回線の使用状況や通信料金を確認してください。

→ ［接続／相手先登録］画面の［使用するタイマ］を「タイマ1、以下の時間帯のみタイマ2に変更」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［タイマ２の時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

→ ［接続／相手先登録］画面の［最大接続時間］を設定していないか確認してください。

→ ［接続／相手先登録］画面の［時間帯による制限］を「以下の時間帯のみ自動接続可能」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［自動接続可能な時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

→ ［接続／相手先登録］画面の［時間帯による着信制限］を「以下の時間帯のみ着信許可」に設定し、［終了時刻で強制切断］をチェックしていると、設定している［着信を許可する時間帯］の終了時刻になると同時に、自動的に回線が切断されます。

■FTPソフトでファイルの送受信ができない

→次のように、FTPソフトの設定を「PASVモード」に変更してください。

・Windows用　NextFTP（Ver.1.91）の場合

［オプション］→［ファイヤーウォール（プロキシ）］タブで［PASVモード］をチェックします。

・Macintosh用　Fetch（Ver.3.0.3J2）の場合

［初期設定］→［Firewall］で［パッシブモード転送（PASV）を使う］をチェックします。

※FTPによるデータ転送は、通常、サーバ側からクライアント側へアクセスした後にデータ転送を開始する仕組みになっています。しかし、本製品の購入時の設定では、外部からの不正なアクセスを防止するため、WAN側から本製品へのアクセスができないようになっています。そのため、FTPサーバからクライアント側へのアクセスもできません。「PASVモード」とは、この現象を回避するため、クライアント側からサーバ側へアクセスするようにした転送方法です。

■Windows Messenger / MSN Messengerで通信ができない

→ 本製品とWindows XP/MeのUPnPの設定を確認してください。Messengerを利用するときは、本製品とWindows XP/MeともにUPnP機能をONする必要があります。

●本製品のUPnP設定をONにする

1. ［詳細設定］→［UPnP設定］をクリックし、［UPnP機能］を［ON］にします。

●Windows XPのUPnP設定をONにする

1. ［スタート］メニューの［コントロールパネル］をクリックし、［ネットワーク接続］をクリックします。
   ［ネットワーク接続］ウィンドウが表示されます。
2. ［詳細設定］メニューから［オプションネットワークコンポーネント］を選択します。
3. コンポーネントの一覧で［ネットワークサービス］をクリックし、［詳細］ボタンをクリックします。
4. ［ネットワークサービス］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。
   チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows XPの画面の指示に従ってください。

●Windows MeのUPnP設定をONにする

1. ［スタート］メニューの［設定］から、［コントロールパネル］をクリックします。
2. ［アプリケーションの追加と削除］アイコンをダブルクリックして、［Windowsファイル］タブをクリックします。
3. ［コンポーネントの種類］で［通信］をクリックし、［詳細］ボタンをクリックします。
4. ［コンポーネントの種類］ダイアログで、［ユニバーサルプラグアンドプレイ］がチェックされているかどうかを確認します。

チェックされていないときは、チェックをつけて［OK］ボタンをクリックします。以降は、Windows Meの画面の指示に従ってください。

→ 通信相手の動作環境を確認してください。通信相手がUPnP対応のルータを使用していますか？または、プライベートIPアドレスを使用しているプロバイダ経由で接続していませんか？このような場合は、Messengerで通信できません。

→ Messengerでの通信がなくなってから、本製品のUPnPポート自動削除設定で設定した時間が経過したときは、自動的に使用されていたポートが閉じます。ポートが閉じてから再びMessengerを使いたいときは、Messengerをいったん終了してから、起動し直してください。Messengerでサインインし直すだけでは正常に動作しませんのでご注意ください。

無線LANのトラブル

■無線通信できない

→ 無線LANカードを挿入したパソコンと本製品のSSIDが一致していない可能性があります。

LAN上のパソコンから本製品の設定ページを開きSSIDを確認し、本製品のSSIDと同じものをパソコン側にも設定してください。

→ 無線LANカードを挿入したパソコンと本製品のWEPキーの設定が一致していない可能性があります。

LAN上のパソコンから本製品の設定ページを開きWEPキーの設定を確認し、本製品のWEPキーと同じものをパソコン側にも設定してください。

→ 本製品やパソコンが、電波の届かない場所にあるか、コンクリートの壁などの障害がある可能性があります。

本製品の近くにパソコンを設置してみてください。

→ 本製品に接続できる端末をMACアドレスの設定によって限定している場合があります。設定を確認してください。

その他のトラブル

■相手先の設定が勝手に変わってしまう

→ ［クイック設定］ページの［PPPoE（端末型）］画面、［PPPoE（LAN型）］画面、［端末型ダイヤルアップ］画面、［フレッツ・ISDN］画面は、［詳細設定］ページの［接続／相手先登録］画面の各相手先番号と共通です。1つの画面で設定を変更すると、他の画面の設定も同じように変更されます。

■パソコンを再起動すると「IPアドレスが使えない」というメッセージが表示される

→［ルータ設定（LAN）］画面の［DHCPサーバ機能］をONにしていますか？

→［ルータ設定（LAN）］画面の［開始IPアドレス/個数］で、Ethernet上の機器より少ない個数を設定していませんか？

→ DHCPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定していますか？

固定する場合、ホスト情報に登録するパソコンのIPアドレスを、DHCPサーバ機能で割り当てることができる範囲内（［ルータ設定（IP設定）］画面の［開始IPアドレス/個数］）で設定してください。

■本製品と通信できない／設定ができない

→パソコンのTCP/IPの設定が正しいか確認してください。→「既存のLAN環境で使用する （1）購入時のIPアドレスのまま導入する」〈P.6〉「既存のLAN環境で使用する （2）本製品のIPアドレスを変更して導入する」〈P.9〉参照

- パソコンのIPアドレスとサブネットマスクは正しく設定していますか？
- パソコンのIPアドレスは、本製品のIPアドレスと同じサブネットワーク番号で設定していますか？
- ゲートウェイは正しく設定されていますか？
- DNSサーバのIPアドレスは正しく設定されていますか？

→ Webブラウザの［オプション］メニューなどで、「プロキシサーバ（あるいはプロクシ）を使用しない」ように設定してください。

- 使用しているWebブラウザの設定で「必要時にインターネットに接続する」などの項目を選択していませんか？
- 使用しているWebブラウザの設定で「プロキシサーバー経由で接続する」などの項目を選択していませんか？

→ WebブラウザのURLを指定する欄に、「http://［本製品のIPアドレス］/」を入力して設定ページを開いてみてください。

開くことができない場合は、パソコンでのIPアドレスの設定が正しいか確認してください。→「既存のLAN環境で使用する （1）購入時のIPアドレスのまま導入する」〈P.6〉、「既存のLAN環境で使用する （2）本製品のIPアドレスを変更して導入する」〈P.9〉参照

→ 設定ページで設定するときにエラーが表示されていないか確認してください。

→ お使いのパソコンがWindowsの場合は、MS-DOSプロンプト画面などでpingを入力して、パソコンと本製品が正しくIP通信しているかどうか確認してください。

→ ルータ機能に関する設定を消去して、最初から設定し直してみてください。

→ ファームウェアを再アップデートしてください。

■本製品の設定をファイルとして保存できない

→ 設定ファイルを保存するとき、ファイルを保存するダイアログでファイルの種類を［HTML］や［HTMLソース］などを選択して保存しましたか？

設定ファイルは、HTML形式にしてください。

■設定ファイルの設定内容を本製品に書き込めない

→ ［本体設定］画面の［本体の名称］の設定を変更したあとで、パソコンを再起動しましたか？

本製品の名前を変更した場合、本製品の名前で設定ファイルを読み込むためには、パソコンを再起動する必要があります。

→ 設定ファイルが壊れている可能性があります。

■設定したパスワードを忘れてしまった

→ 本体のリセットスイッチを使って、ルータ機能の設定を購入時の状態に戻してください。詳しくは、導入／設定マニュアル「ルータ機能の設定を購入時の状態に戻すには」を参照してください。

2 設定ページのエラー一覧

［接続／相手先登録］画面から手動で相手先に接続しようとした場合にエラーメッセージが表示されたときや、［情報表示（接続／切断ログ）］画面にエラーが表示されているときは、下記を参照して対処してください。

MN128-SOHO ISDN網エラー

●［網理由表示＃６：チャネル利用不可］

→ 相手先がISDN回線を使用しているか確認してください。

●［網理由表示＃17：着ユーザビジー］

→ 相手先のISDN回線のBチャネルが空いていません。しばらく待ってから、再発信してください。

●［網理由表示＃18：着ユーザレスポンスなし］

→ 相手先が応答しません。
［接続相手先登録］画面の［相手先電話番号］を確認してください。

→ 相手先の端末が正しく接続されているか確認してください。

●［網理由表示＃20：加入者不在］

→ しばらく待ってから、再発信してください。

→ 相手先が応答しません。
［接続／相手先登録］画面の［相手先電話番号］を確認してください。

●［網理由表示＃21：通信拒否］

→ 相手先に接続を拒否されました。
相手先が着信を許可しているか確認してください。

●［網理由表示＃27：相手端末故障中］

→ 相手先に次のことを確認してください。
・端末の電源をONにしていますか？
・各機器を正しく接続していますか？

●［網理由表示＃28：無効番号フォーマット（不完全番号）］

→ ［接続／相手先登録］画面の［相手先電話番号］を確認してください。

● ［網理由表示＃34：利用可回線／チャネルなし］

→ ほかの端末によって使用されているため、こちら側のISDN回線のBチャネルが空いていません。Bチャネルが空いてから、再発信してください。

● ［網理由表示＃41：一時的障害］

→ しばらく待ってから、再発信してください。

● ［網理由表示＃44：要求回線／チャネル利用不可］

→ 相手先のISDN回線のBチャネルが空いていません。相手先のBチャネルが空いてから、再発信してください。

● ［網理由表示＃88：端末属性不一致］

→ 相手先の属性が異なります。
相手先と属性が一致しているか確認してください。

→ 電話機やファクシミリなどが応答しました。
［接続／相手先登録］画面の［相手先電話番号］を確認してください。

→ 相手先に次のことを確認してください。
・各機器は正しく接続していますか？
・各機器にサブアドレスを正しく設定していますか？

MN128-SOHO PPPエラー

● ［PPPエラー：認証プロトコル不一致］

→ ［接続／相手先登録］画面の［認証プロトコル］を変更して、再発信してください。

● ［PPPエラー：認証失敗］

→ IDまたはパスワードが間違っています。
［接続／相手先登録］画面の［送信ユーザID］［送信パスワード］に正しいIDおよびパスワードを設定して、再発信してください。

→ 暗号化の設定が間違っています。
・MPPEで暗号化したデータをやり取りする場合は、［接続／相手先登録］画面で次の設定を確認してください。
［認証プロトコル］は［MS-CHAPv2］を選択する
［暗号化］で［MPPE-40］または［MPPE-128］のどちらかを選択（双方で同じものを選択してください。）なお、どちらかで［MPPE-any］を選択しても構いません。

・本製品独自の暗号化したデータをやり取りする場合は、双方で［接続／相手先登録］画面の［暗号化］を「独自」、［鍵配送鍵］に同じ文字列を設定して、再発信してください。

●［PPPエラー：接続要求再送タイムアウト］

→ 本製品を再起動して、再発信してください。

●［PPPエラー：認証再送タイムアウト］

→ 本製品を再起動して、再発信してください。

●［PPPエラー：プロトコル拒否］

→ 本製品を再起動して、再発信してください。

→ 相手先がIP通信をサポートしていない場合があります。
相手先の通信プロトコルを確認してください。

●［PPPエラー：コールバック要求失敗］

→ コールバックできません。
［接続／相手先登録］画面の［コールバック発信］で［なし］を選択してください。

●［PPPエラー：割り当てIPアドレスなし］

→ リモートアクセスを受ける側の場合は、［ルータ設定（LAN）］画面の［リモートアクセスサーバ機能］を［ON］に、リモートアクセスを許可する側の場合は、［リモートIPアドレス1/2/3/4］にリモートアクセス用のIPアドレスを設定してください。

→ こちらから発信したときにこのメッセージが表示される場合は、次のことを確認してください。
- 相手先はリモートアクセスを許可していますか？
- 相手先を登録している［接続／相手先登録］画面の［接続モード］で［端末型接続］を選択してください。

●［PPPエラー：LCP接続要求再送タイムアウト］

→［接続／相手先登録］画面の［通信チャネル］を変更してください。

●［PPPエラー：LCP接続失敗］

→［接続／相手先登録］画面の［通信チャネル］を変更してください。

●［PPPエラー：CBCP不許可］

→ コールバックできません。
［接続／相手先登録］画面の［コールバック発信］で［なし］を選択してください。

●［PPPエラー：IPCP接続要求再送タイムアウト］

→［接続／相手先登録］画面の［接続モード］を変更してください。

→ 相手先がIPプロトコルをサポートしているか、確認してください。

●［PPPエラー：IPCP接続失敗］

→［接続／相手先登録］画面の［接続モード］を変更してください。

→ 相手先がIPプロトコルをサポートしているか、確認してください。

3 クイック設定で自動的に設定されるフィルタ

クイック設定で、接続の設定を行うと［ルータ設定（LAN）］画面のオプション欄に次のフィルタが自動的に設定されます。
※フィルタ番号は異なる場合があります。

［ブロードバンドで設定］→［PPPoE端末型］

下記のフィルタで、「remote 0」のフィルタは「メイン：接続相手先登録#0」を設定すると追加されます。「remote 1」のフィルタは「メイン（予備）：接続相手先登録#1」を設定すると追加されます。「wannay」のフィルタはクイック設定すると、必ず設定されるフィルタです。なお、サブセッション（接続相手先登録#2～#7）を設定した場合は、「wanany」のフィルタのみ適用されます。

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany

フィルタ#57によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#58によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（“pass in”）を登録してください。

● WAN（Ethernet）側からの送信元IPアドレスが不正なパケットを破棄するフィルタ

ip filter 43 reject in 10.0.0.0/8 * * * * remote 0
ip filter 44 reject in 172.16.0.0/12 * * * * remote 0
ip filter 45 reject in 192.168.0.0/16 * * * * remote 0
ip filter 46 reject in 10.0.0.0/8 * * * * remote 1
ip filter 47 reject in 172.16.0.0/12 * * * * remote 1
ip filter 48 reject in 192.168.0.0/16 * * * * remote 1
ip filter 49 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスの不正なパケットがWAN（Ethernet）側へ送るのを防止するフィルタ

ip filter 47 reject out * 10.0.0.0/8 * * * remote 0
ip filter 48 reject out * 172.16.0.0/12 * * * remote 0
ip filter 49 reject out * 192.168.0.0/16 * * * remote 0
ip filter 53 reject out * 10.0.0.0/8 * * * remote 1
ip filter 54 reject out * 172.16.0.0/12 * * * remote 1
ip filter 55 reject out * 192.168.0.0/16 * * * remote 1
ip filter 57 reject out * 〈本体の属するネットワークアドレス〉/24 * * * wanany
ip filter 59 reject out * 169.254.0.0/16 * * * wanany

フィルタ#47、#48、#53、#54は本体に設定されているIPアドレスがグローバルIPアドレスの時のみ設定されます。
本体をリモートアクセスサーバとして使用する場合はこのフィルタを削除するか、ま

たは必要に応じてフィルタを追加してください。
フィルタが設定されたあとに本体のIPアドレスを変更した場合は、そのIPアドレスにあわせてフィルタを設定し直してください。

● LAN上にWindows 2000 Serverがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 60 reject dns qtype 6

● LAN上にWindows XP/2000/98 SE/Meがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 *wanany
ip filter 64 restrict out * * udp 137 domain wanany

このフィルタによりこのままではMicrosoftネットワークを利用して相手先の共有フォルダにアクセスができなくなる場合がありますので、必要に応じて削除してください。
"tcpfin"は、TCPセッションの終了（FIN）パケット及びリセット（RST）パケットのみを対象とします。

[ブロードバンドで設定] → [PPPoE LAN型]

下記のフィルタで、「remote 0」のフィルタは「メイン：接続相手先登録#0」を設定すると追加されます。「wannay」のフィルタはクイック設定すると、必ず設定されるフィルタです。なお、サブセッション（接続相手先登録#2〜#7）を設定した場合は、「wanany」のフィルタのみ適用されます。
※「メイン（予備）：接続相手先登録#1」を設定すると「remote 1」のフィルタが追加されます。

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 63 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 64 reject in * * tcpest * * wanany

フィルタ#63によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#59によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（‘ pass in ’）を登録してください。

● WAN（Ethernet）側からの送信元IPアドレスが不正なパケットを破棄するフィルタ

ip filter 45 reject in 10.0.0.0/8 * * * * remote 0
ip filter 46 reject in 172.16.0.0/12 * * * * remote 0
ip filter 47 reject in 192.168.0.0/16 * * * * remote 0
ip filter 48 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスの不正なパケットがWAN（Ethernet）側へ出るのを防止するフィルタ

ip filter 49 reject out * 10.0.0.0/8 * * * remote 0
ip filter 50 reject out * 172.16.0.0/12 * * * remote 0
ip filter 51 reject out * 192.168.0.0/16 * * * remote 0
ip filter 52 reject out * 〈本体の属するネットワークアドレス〉/24 * * * wanany
ip filter 53 reject out * 169.254.0.0/16 * * * wanany

フィルタ#49、#50は本体に設定されているIPアドレスがグローバルIPアドレスの時のみ設定されます。
本体をリモートアクセスサーバとして使用する場合はこのフィルタを削除するか、または必要に応じてフィルタを追加してください。
フィルタが設定されたあとに本体のIPアドレスを変更した場合は、そのIPアドレスにあわせてフィルタを設定し直してください。

● RIPのDirected-Broadcastに関するフィルタ

ip filter 59 pass in * 〈本体の属するネットワークアドレス〉/32 udp route route remote 0 nolog
ip filter 60 pass in * 〈本体の属するブロードキャストアドレス〉/32 udp route route remote 0 nolog
ip filter 61 reject in * 〈本体の属するネットワークアドレス〉/32 * * * remote 0
ip filter 62 reject in * 〈本体の属するブロードキャストアドレス〉/32 * * * remote 0

● LAN上にWindows 2000 Serverがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 54 reject dns qtype 6

● LAN上にWindows XP/2000/98 SE/Meがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 55 restrict out * * tcpfin * * wanany
ip filter 56 restrict out * * * * 137-139 wanany
ip filter 57 restrict out * * * 137-139 * wanany
ip filter 58 restrict out * * udp 137 domain wanany

このフィルタによりこのままではMicrosoftネットワークを利用して相手先の共有フォルダにアクセスができなくなる場合がありますので、必要に応じて削除してください。
"tcpfin"は、TCPセッションの終了（FIN）パケット及びリセット（RST）パケットのみを対象とします。

[ブロードバンドで接続] → [DHCP] / [Static]

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany
フィルタ#58によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#59によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（‘pass in’）を登録してください。

● WAN（Ethernet）側からの送信元IPアドレスが不正なパケットを破棄するフィルタ

ip filter 49 reject in 10.0.0.0/8 * * * * wanether
ip filter 50 reject in 172.16.0.0/12 * * * * wanether
ip filter 51 reject in 192.168.0.0/16 * * * * wanether
ip filter 52 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスが不正なパケットがWAN（Ethernet）側へ出るのを防止するフィルタ

ip filter 53 reject out * 10.0.0.0/8 * * * wanether
ip filter 54 reject out * 172.16.0.0/12 * * * wanether
ip filter 55 reject out * 192.168.0.0/16 * * * wanether
ip filter 56 reject out * 〈本体の属するネットワークアドレス〉 * * * wanany
ip filter 59 reject out * 169.254.0.0/16 * * * wanany
フィルタ#53、#54は本体に設定されているIPアドレスがグローバルIPアドレスの時のみ設定されます。
本体をリモートアクセスサーバとして使用する場合はこのフィルタを削除するか、または必要に応じてフィルタを追加してください。
フィルタが設定されたあとに本体のIPアドレスを変更した場合は、そのIPアドレスにあわせてフィルタを設定しなおしてください。

● LAN上にWindows 2000 Serverがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 60 reject dns qtype 6

● LAN上にWindows XP/2000/98 SE/Meがあるときに発生する、「意図しない自動接続」を防止するためのフィルタ（工場出荷時の状態で設定されています。設定を全て初期化した場合にも自動的に設定されます。）

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

このフィルタによりこのままではMicrosoftネットワークを利用して相手先の共有フォルダにアクセスができなくなる場合がありますので、必要に応じて削除してください。
"tcpfin"は、TCPセッションの終了（FIN）パケット及びリセット（RST）パケットのみを対象とします。

[ISDNで接続] → [端末型ダイヤルアップ]

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany

フィルタ#58によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#59によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（‘pass in’）を登録してください。

● WAN側からの送信元IPアドレスが不正なパケットを破棄するためのフィルタ

ip filter 49 reject in 10.0.0.0/8 * * * * remote 0
ip filter 50 reject in 172.16.0.0/12 * * * * remote 0
ip filter 51 reject in 192.168.0.0/16 * * * * remote 0
ip filter 52 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスの不正なパケットがWAN側へ出るのを防止するためのフィルタ

ip filter 53 reject out * 10.0.0.0/8 * * * remote 0
ip filter 54 reject out * 172.16.0.0/12 * * * remote 0
ip filter 55 reject out * 192.168.0.0/16 * * * remote 0
ip filter 56 reject out * 〈本体の属するネットワークアドレス〉/24 * * * wanany
ip filter 59 reject out * 169.254.0.0/16 * * * wanany

フィルタ#53、#54は、本体に設定されているIPアドレスがグローバルIPアドレスの場合のみ設定されます。本体をリモートアクセスサーバとして使用する場合は、このフィルタを削除するか、必要なフィルタを追加してください。フィルタが設定された後に本体のIPアドレスを変更した場合は、新しいIPアドレスに合わせてフィルタを設定し直してください。

● LAN上にWindows 2000 Serverがあるときに起こる「意図しない自動接続」を防止するためのフィルタ

ip filter 60 reject dns qtype 6

● Webブラウザを終了するときに起こる「意図しない自動接続」を防止するためのフィルタ

ip filter 61 restrict out * * tcpfin * * wanany

※「tcpfin」は、TCPセッションの終了（FIN）パケットおよびリセット（RST）パケットを対象とします。

● Windows XP/2000/98 SE/Meが行う定期的な通信によって起こる「意図しない自動接続」を防止するためのフィルタ：

ip filter 61 restrict out * * tcpfin * * wanany
ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

[ISDNで接続] → [フレッツ・ISDN]

下記のフィルタで、「remote 0」のフィルタは「メイン：接続相手先登録#0」を設定すると追加されます。「remote 1」のフィルタは「メイン（予備）：接続相手先登録#1」を設定すると追加されます。「wannay」のフィルタはクイック設定すると、必ず設定されるフィルタです。なお、サブセッション（接続相手先登録#2〜#7）を設定した場合は、「wanany」のフィルタのみ適用されます。

● WAN（Ethernet）側からの不正アクセスを防止するフィルタ

ip filter 57 reject in * 〈本体のIPアドレス〉/32 tcpest * * wanany
ip filter 58 reject in * * tcpest * * wanany

フィルタ#58によって、WAN側から本製品へアクセスすることができなくなります。とくに必要がない限り、削除しないでください。
フィルタ#59によって、WAN側からTCPのセッションをオープンすることができなくなります。LAN上のサーバを外部に公開する場合などは、このフィルタを削除するか、WAN側からアクセスできるフィルタ（“pass in”）を登録してください。

● WAN側からの送信元IPアドレスが不正なパケットを破棄するためのフィルタ

ip filter 43 reject in 10.0.0.0/8 * * * * remote 0
ip filter 44 reject in 172.16.0.0/12 * * * * remote 0
ip filter 45 reject in 192.168.0.0/16 * * * * remote 0
ip filter 46 reject in 10.0.0.0/8 * * * * remote 1
ip filter 47 reject in 172.16.0.0/12 * * * * remote 1
ip filter 48 reject in 192.168.0.0/16 * * * * remote 1
ip filter 49 reject in 〈本体の属するネットワークアドレス〉/24 * * * * wanany

● 送信先IPアドレスの不正なパケットがWAN側へ出るのを防止するためのフィルタ

ip filter 50 reject out * 10.0.0.0/8 * * * remote 0
ip filter 51 reject out * 172.16.0.0/12 * * * remote 0
ip filter 52 reject out * 192.168.0.0/16 * * * remote 0
ip filter 53 reject out * 10.0.0.0/8 * * * remote 1
ip filter 54 reject out * 172.16.0.0/12 * * * remote 1
ip filter 55 reject out * 192.168.0.0/16 * * * remote 1
ip filter 56 reject out * 〈本体の属するネットワークアドレス〉/24 * * * wanany
ip filter 59 reject out * 169.254.0.0/16 * * * wanany

フィルタ#50、#51、#53、#54は、本体に設定されているIPアドレスがグローバルIPアドレスの場合のみ設定されます。本体をリモートアクセスサーバとして使用する場合は、このフィルタを削除するか、必要に応じてフィルタを追加してください。
フィルタが設定された後に本体のIPアドレスを変更した場合は、新しいIPアドレスに合わせてフィルタを設定し直してください。

● LAN上にWindows2000 Serverがあるときに起こる「意図しない自動接続」を防止するためのフィルタ：

ip filter 60 reject dns qtype 6

● Webブラウザを終了するときに起こる「意図しない自動接続」を防止するためのフィルタ

ip filter 61 restrict out * * tcpfin * * wanany

※「tcpfin」は、TCPセッションの終了（FIN）パケットおよびリセット（RST）パケットを対象とします。

● Windows XP/2000/98 SE/Meが行う定期的な通信によって起こる「意図しない自動接続」を防止するためのフィルタ

ip filter 62 restrict out * * * * 137-139 wanany
ip filter 63 restrict out * * * 137-139 * wanany
ip filter 64 restrict out * * udp 137 domain wanany

これらのフィルタによって、相手先の共有フォルダを利用する際に、Microsoftネットワークを利用できなくなることがあります。必要に応じて削除してください。
※フィルタ番号は異なる場合があります。

4 お問い合わせ先

メンテナンスサービスについて

- 本製品に含まれるソフトウェアが保存されている媒体に欠陥があった場合、お買い上げの販売代理店または小売店に返却してください。無償にて新品と交換いたします。なお、欠陥品送付にともなう送料は、送り主負担とさせていただきます。
- 本製品に含まれるハードウェアが購入後、１年間に通常のご使用において故障した場合、これを保証します。故障品に保証書を添えて、お買い上げの販売代理店または小売店に返却してください。無償にて修理いたします。なお、修理品送付にともなう送料は、送り主負担とさせていただきます。
- 保証期間でも次のような場合には、有償修理になります。

  (1) 保証書のご提示がない場合

  (2) 保証書に機器の製造番号、ご購入日、販売店名の記入がない場合、または字句を書き替えられた場合

  (3) 接続しているほかの機器に起因して生じた故障、または不当な修理や改造、調整をされた場合

  (4) 使用上の誤り、または故意・他意に関わらず、ほかの要因による損傷および故障の場合

  (5) 火災、地震、風水害、落雷、そのほかの天災地変、公害や異常電圧による損傷および故障の場合

  (6) 購入後の輸送、移動時の落下など、お取り扱いが不適当なため生じた損傷および故障の場合

  (7) 購入後の取り付け場所の移動、落下などにより生じた損傷および故障の場合

お問い合わせ先

本製品について技術的なご質問、または製品アップグレードに関するご質問は、お買い上げの販売代理店、小売店、またはMNテクニカルセンタまでお問い合わせください。

MNテクニカルセンタ

TEL：0570−055−128（NTT 一般電話、携帯電話用）
　　　03−5550−8420（PHS、およびNTT以外の電話用）
FAX：0570−056−128

※9:40〜17:50（土・日・休日・年末年始は除く）
※FAXは24時間受け付けております。

ホームページのご案内

株式会社エヌ・ティ・ティ エムイーのホームページにて、製品のサポート情報、マニュアル、最新のファームウェア、アプリケーションなどを提供する予定ですので、ご活用ください。

・株式会社エヌ・ティ・ティ エムイー「MN128 Information」
http://www.ntt-me.co.jp/mn128/

ブロードキャストアドレス

ブロードキャストとは、ネットワークまたはサブネット内の、全ノードが受け取るべきパケットを送ることを指します。この際、パケットの送り先に指定するIPアドレスを、ブロードキャストアドレスといいます。ブロードキャストアドレスは、ネットワーク上の全ノードのIPアドレスと重複しない値を任意に設定できますが、通常は、将来的なノードの追加の際にアドレス割り当てが容易になるよう、または経路制御を把握しやすくするため、以下の方法がとられます。

▼ ネットワーク内の全ホストブロードキャストの設定

- サブネットを設定していない場合（ネットワーク番号は固有の値、ホスト部のビットがすべて１<10進数で255>）
  例）クラスB、IPアドレスのネットワーク番号が「172.16.X.X」の場合
  →ブロードキャストアドレスは「172.16.255.255」
- サブネットを設定している場合（ネットワーク番号は固有の値、サブネット部、ホスト部のビットがすべて１）
  例） クラスB、IPアドレスのネットワーク番号が「172.16.X.X」、サブネットマスクが「255.255.255.0」の場合
  →ブロードキャストアドレスは「172.16.255.255」

▼ 特定のサブネット内に適用されるブロードキャストの設定

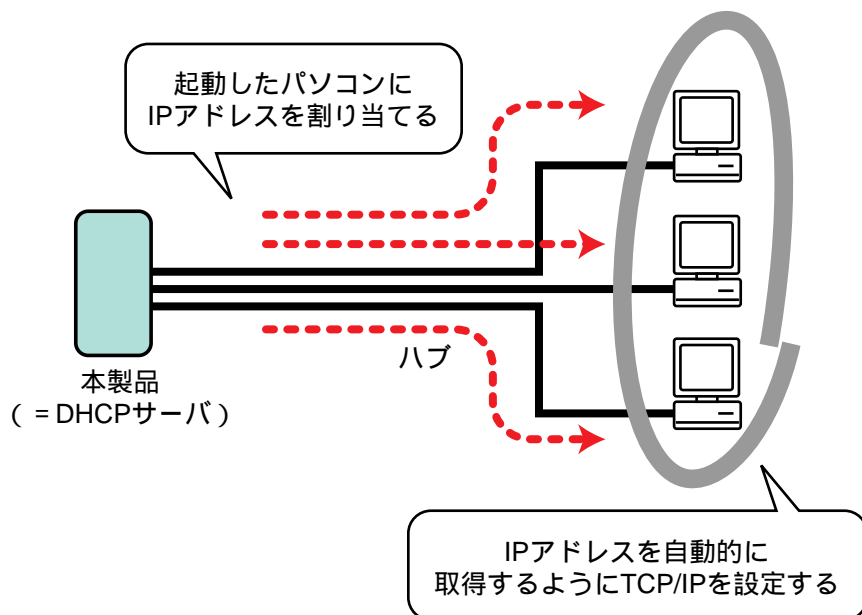
（ネットワーク番号、サブネット部は固有の値、ホスト部のビットがすべて１）
例） クラスB、IPアドレスのネットワーク番号が「172.16.X.X」、サブネットマスクが「255.255.255.0」「172.16.15.X」のサブネットのみにブロードキャストする場合
→ブロードキャストアドレスは「172.16.15.255」

デフォルトルータアドレス

送り先不明のパケットが送られるルータを「デフォルトルータ」といいます。
また、デフォルトルータを示すIPアドレスのことを「デフォルトルータアドレス」といいます。
各ルータがパケットを受け取ったあと、送り先アドレスのノードがないなど送り先がわからない場合に、各ルータはデフォルトルータへパケットを送ります。
インターネットに接続されているネットワークには、必ず１つのデフォルトルータが必要です。同一ネットワークに複数のルータがある場合は、どれか１つをデフォルトルータにしてください。

DHCPサーバ/BOOTPサーバ機能

本製品には、DHCPサーバとして働く「DHCP/BOOTPサーバ機能」が搭載されています。

通常、DHCPサーバはIPを利用したネットワーク（IPネットワーク）で必要な設定を一元管理し、起動したDHCPクライアントに設定情報を与えます。与えられる設定情報には、IPアドレス、サブネットマスク、ルータのIPアドレス、DNSサーバのIPアドレス、ドメイン名などが含まれています。
DHCPクライアントはIPネットワークで必要な設定情報をすべてDHCPサーバから与えられます。したがって、DHCPクライアントがDHCPサーバの存在するネットワーク間を移動しても、IPネットワークに関する設定を変更する必要がありません。

本製品を使用しているLAN上のパソコンは、TCP/IPの設定で「IPアドレスを自動的に取得する」ように指定すると、本製品のDHCPクライアントになります。DHCPクライアントは起動すると、動的にDHCPサーバである本製品からIPアドレスなどの設定情報を与えられます。
なお、MacTCPなどBOOTPにしか対応していないパソコンも、動的に本製品からIPアドレスを割り当てられます。ただし、ドメイン名など一部の設定情報は与えられません。

◆割り当てられたIPアドレス

DHCP/BOOTPサーバ機能で割り当てられたIPアドレスは、[ルータ設定（LAN）] 画面の［リース時間］で設定された時間が経過するまで使用されます。本製品のIPアドレスの変更に伴ってパソコンのIPアドレスの変更が必要な場合でも、一度設定されたIPアドレスは自動的に更新されません。
パソコンに新しいIPアドレスを設定する必要がある場合は、それぞれのパソコンで操作してください。詳しくは、「IPアドレスの再取得方法について」〈P.17〉を参照してください。

◆割り当てるIPアドレスとパソコンの組み合わせを固定する
DHCP/BOOTPサーバ機能を使ってパソコンのIPアドレスを設定する際、パソコンと設定するIPアドレスの組み合わせを固定できます。あらかじめ本製品にパソコンのホスト名と対応するIPアドレスの組み合わせを登録します。
詳しくは、**「DHCP/BOOTPサーバ機能で割り当てるIPアドレスとパソコンの組み合わせを固定する」〈P.24〉を参照してください。**

AutoNAT機能

本製品には、「NAT」と「IP Masquerade」に対応した「AutoNAT機能」が搭載されています。
AutoNAT機能によって、プロバイダとPPPoE端末型または端末型ダイヤルアップで接続しているときでも、LAN側の複数台のパソコンが同時にインターネットを利用できます。この際、出荷時の設定を変更する必要はありません。なお、同時に接続できる台数に制限はありませんが、同時に行うことができるセッションは「256」までです。

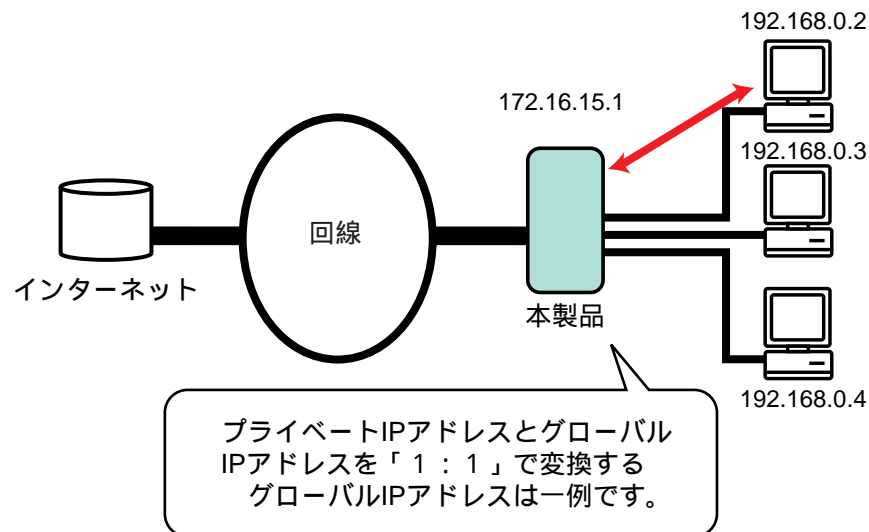
また、変換するプライベートIPアドレスとグローバルIPアドレスの組み合わせを固定したいときは、IPアドレス変換（NAT）テーブルを登録します。
IPアドレス変換（NAT）テーブルを登録すると、次のような接続形態を実現できます。

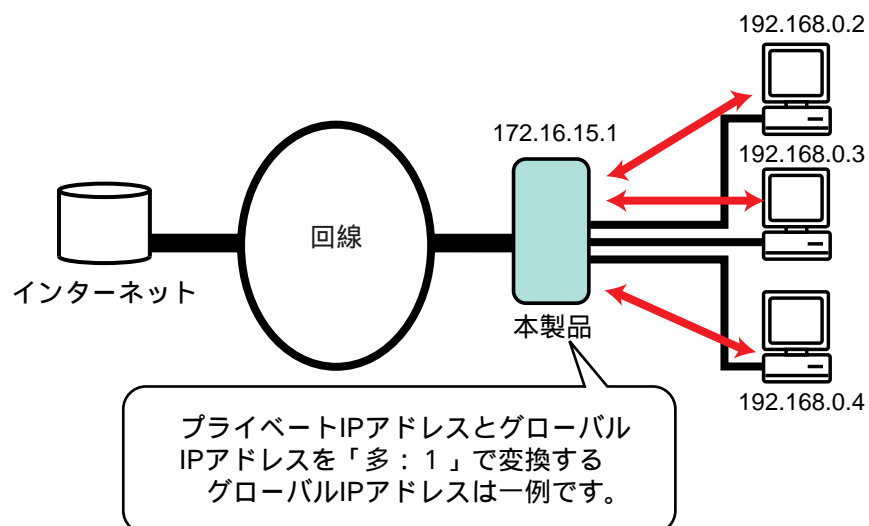
- **WAN側にアクセスできるLAN側のパソコンを限定する**
- **WAN側からアクセスできるLAN側のパソコンを限定する**
- **WAN側からLAN側にアクセスできないようにする**

IPアドレス変換（NAT）テーブルは、設定ページの［ルータ設定（LAN)］画面のオプション欄で必要に応じて登録します。
PPPoE端末型または端末型ダイヤルアップ接続時にIPアドレス変換（NAT）テーブルもフィルタも登録していないときは、LAN側のすべてのパソコンがインターネットを利用できます。ただし、WAN側からLAN側にアクセスすることはできません。

NATとIP Masquerade、それぞれの機能を補足します。

▼NAT

NATとは、LAN側で使用しているプライベートIPアドレスとWAN側で使用しているグローバルIPアドレスを変換する機能です。NATによって、LAN側のパソコンに設定されているプライベートIPアドレスは自動的にグローバルIPアドレスに変換され、WAN側に接続できるようになります。IPアドレスを手動で変更する必要はありません。
しかし、NATは１つのプライベートIPアドレスを１つのグローバルIPアドレスに変換することしかできません。したがって、プロバイダにPPPoE端末型接続、または端末型ダイヤルアップ接続するときなどグローバルIPアドレスが１つしか割り当てられない場合、インターネットを利用できるLAN側のパソコンは１台だけになります。

▼IP Masquerade

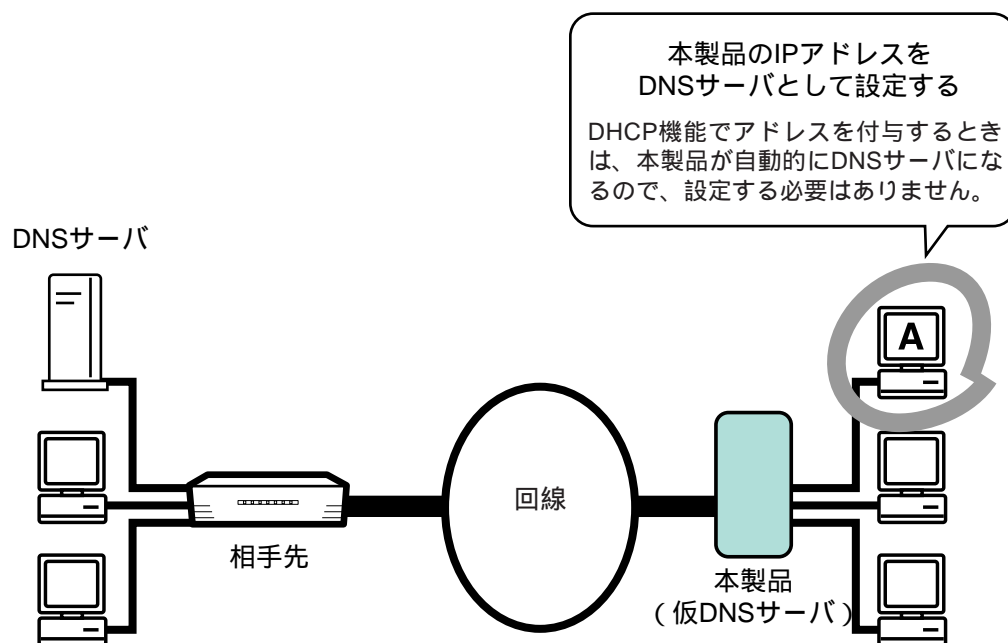
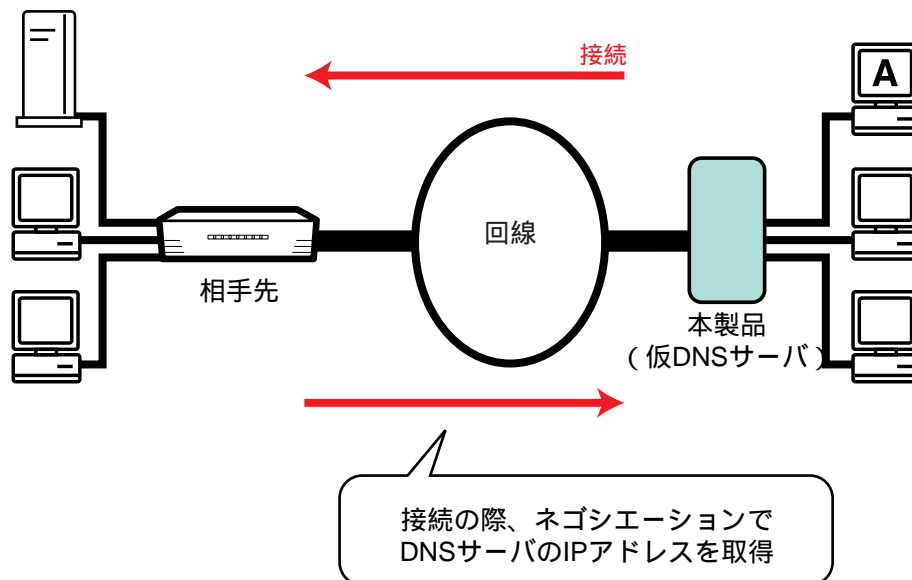
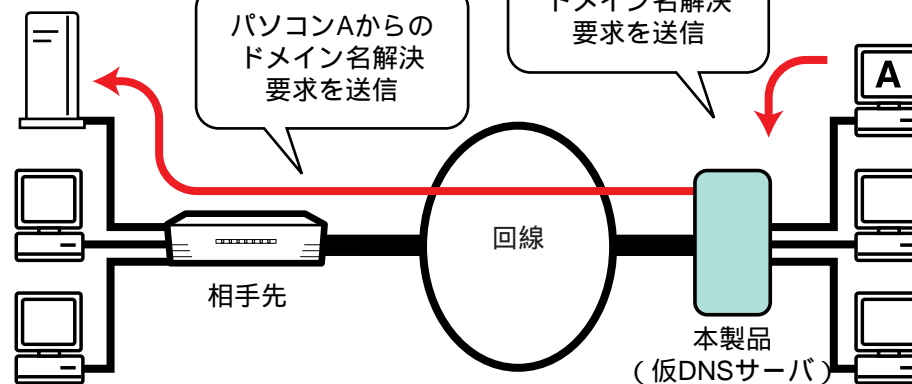
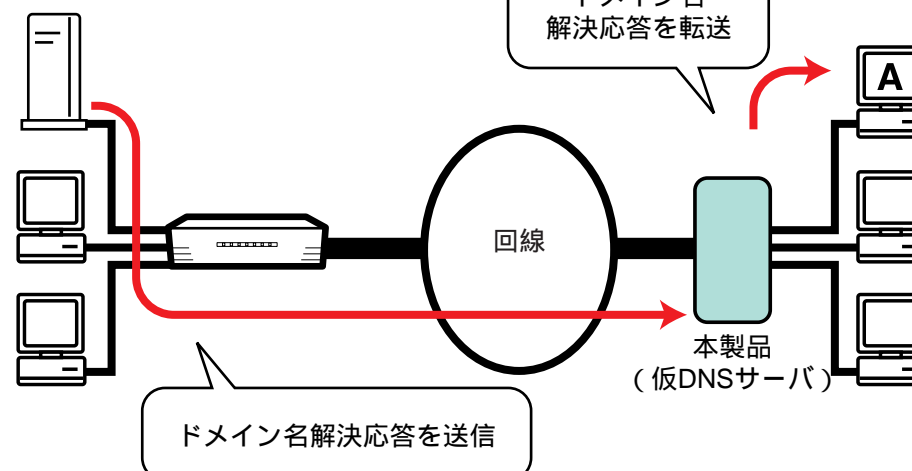
IP Masqueradeとは、LAN側で使用している複数のプライベートIPアドレスとWAN側で使用している1つのグローバルIPアドレスを対応付けする機能です。IP Masqueradeによって、プロバイダに端末型ダイヤルアップ接続するときなどグローバルIPアドレスが1つしか割り当てられない場合でも、LAN側の複数台のパソコンが同時にインターネットを利用できるようになります。

AutoDNS機能

本製品には、ドメインネームサービス（DNS）サーバのIPアドレスの自動取得とDNSの代理応答をする「AutoDNS機能」が搭載されています。
AutoDNS機能によって、PPPoE端末型または端末型ダイヤルアップ接続する相手先を変更しても、LAN上のパソコンのDNSサーバのIPアドレスの設定を変える必要がなくなります。

AutoDNS機能を使うには、LAN上のパソコンでDNSサーバとして本製品のIPアドレスを設定します。設定後、パソコンから本製品に、ドメイン名を解決するための要求（ドメイン名解決要求）が送信されるようになります。ドメイン名解決要求を受信した本製品は、自動的に次の相手先からDNSサーバのIPアドレスを取得します。

- LAN側のDNSサーバを指定している場合はそのDNSサーバから（※注）
- すでに回線を接続している場合はその相手先から
- 回線をまだ接続していない場合は、自動接続先に接続後、その相手先から
（自動接続先の設定をしていないときは、回線を接続するまでDNSサーバのIPアドレスを取得できません）

自動接続先を設定している場合、LAN側のDNSサーバがドメイン名を解決できないと送信したときは、自動接続先に接続します。LAN側のDNSサーバが何も応答を送信しないときは、自動接続しません。

1. パソコンでDNSサーバのIPアドレスを設定

2. DNSサーバのIPアドレス取得

3. DNS代理応答

本製品はDNSサーバのIPアドレスを自動取得したあと、そのDNSサーバにドメイン名解決要求を送信します。DNSサーバから本製品にドメイン名解決要求に対する応答（ドメイン名解決応答）が送信されると、本製品はパソコンにそのドメイン名解決応答を転送します。これでDNSの代理応答が完了します。

なお、相手先によっては自動的にDNSサーバのIPアドレスを取得できないことがあります。その場合は、接続したい相手先を登録している設定ページの［接続／相手先登録］画面の［DNSサーバアドレス］に相手先のDNSサーバのアドレスを入力してください。

◆本製品を簡易DNSサーバにする
AutoDNS機能を使うとき、本製品を簡易DNSサーバとして使用できます。あらかじめ本製品にパソコンのホスト名と対応するIPアドレスの組み合わせを登録します。
詳しくは、「簡易DNSサーバにする」〈P.22〉を参照してください。

なお、パソコンから送信されたドメイン名解決要求は、次の順に検索されます。

1）本製品に設定されているホスト情報
2）LAN側のDNSサーバ（［ルータ設定（LAN)］画面の［LAN側DNSサーバアドレス］で設定しているときだけ）
3）相手先のDNSサーバ（回線を接続しているとき、または、［自動接続相手先］画面で自動接続先を設定しているときだけ）

VPN（Virtual Private Network）

VPNとは、インターネットなどの公衆網上で論理的なグループを構成し、そのグループ間で閉域性を保つ仕組みを設けたネットワークのことです。公衆網には不特定多数のユーザが接続していますが、VPNを実現することによって、特定のユーザの間だけの通信が可能になります。
専用回線やISDN回線を利用する場合、その通話料金は接続距離に比例するため、遠隔地に接続するときほど料金が高くなります。一方、インターネットの利用料金は、アクセス回線の速度や接続時間に依存します。したがって、送信元と送信先がインターネットに接続している場合は、インターネットを経由して送信元と送信先を接続すると、比較的安い料金で通信を行うことができます。VPNを構築すると、このようにインターネットを介して送信元と送信先のネットワークを接続するということが実現できます。
インターネット上でのセキュリティに関しては、VPNに対応している機器がIPsec、PPTP、L2TPなどの技術を使って、ユーザ認証を行うことで権利のないユーザからの不正アクセスを防いでいます。

PPTP（Point to Point Tunneling Protocol）

PPTPはPPPパケットをIPパケットでカプセル化して、IPネットワークに通すことを可能にするプロトコルで、PPPパケットを通すためのトンネル（Tunneling）の役割を果たします。また、カプセル化するIPパケットにユーザIDやパスワードなどの認証用データを格納して送信するので、送信元と送信先でのユーザ認証が実現できます。なお、送信元と送信先では共にPPTPに対応している機器が必要です。
PPTPを使うと、LANなどのプライベートネットワークから、インターネットを利用し遠隔地にある別のネットワークへデータを送信するなど、VPNが実現できます。

Windowsの場合、お使いのダイヤルアップネットワークのバージョンによっては、ダイヤルアップネットワークを利用してPPTPクライアントになり、PPTPサーバにアクセスすることができます。

IPsec（Security Architecture for Internet Protocol）

IPsecは、暗号通信のための規格の1つです。IPのパケットを暗号化して送受信するので、TCPやUDPなど上位のプロトコルを利用するさまざまなサービスを保護できます。IPsecは、通信を行う上でのセキュリティを確保するために、「機密性の確保」「完全性の確保」「送信元の確保」「否認の防止」が守れるように設計されています。これにより、PPTPよりもセキュリティが強固なVPNを実現できます。

IPsecそのものはひとつのプロトコルではなく、複数のプロトコルで構成されています。それらの中で中核をなすのは次の3つです。

- 認証ヘッダ（AH Authentication Header）
  パケット内のデータの改ざんを防止するためのパケット認証を行います。
- 暗号ペイロード（ESP Encapsulating Security Payload）
  認証と暗号化までを行います。
- IKE（Internet Key Exchange）
  暗号・認証のパラメータを動的に生成して、鍵交換を行います。

L2TP（Layer2 Tunneling Protocol）

L2TPは、Microsoft社が提唱した「PPTP」とCisco Sytems社が開発した「L2F」の2つのプロトコルの仕様をもとに開発された、PPP通信をトンネリングするためのデータリンク層のプロトコルです。基本的な考え方はPPTPと同様、PPPのパケットをトンネリングで運ぶもので、もともとインターネットプロバイダがVPNサービスに利用することが想定されていました。
L2TPは暗号化機能が実装されていないので、IPsecと組み合わせた利用方法が一般的です。

6 用語解説

ADSL（Asymmetric Digital Subscriber Line）

上り方向と下り方向の通信速度が非対称な高速データ通信技術です。すでに一般家庭に普及している電話線を使って、インターネットへの高速で安価な常時接続環境を提供します。

APOP（Authenticated Post Office Protocol）

POPを利用してメールサーバ（POPサーバ）に接続する際に、使用するパスワードを毎回暗号化してユーザを認証する方法です。パスワードをそのまま送信するPOPより、セキュリティの高い方法といえます。

BACP（Bandwidth Allocation Control Protocol）

複数のチャネルを用いたMP通信で、リンクするチャネル数を制御するプロトコルです。MPで通信中にスループットBOD機能を用いて使用するチャネル数を自動的に変更するとき、チャネル数を変更してもよいかを接続先に問い合わせたり、接続先からチャネル数の変更を要求された場合に変更を許可するかどうかを接続先に知らせます。
BACPのプロトコル自体は、接続時にBACPに対応しているかどうかの確認だけに使用されます。実際に、使用するチャネル数の変更を接続先に要求したり、接続先からの要求に答える場合は、BAP（Bandwidth Allocation Protocol）が使用されます。

BAP（Bandwidth Allocation Protocol）

MPで通信中にスループットBOD機能を用いて使用するチャネル数を自動的に変換するとき、実際に接続先に使用するチャネル数の変更を要求したり、接続先から受けた要求に答えるプロトコルです。

BOOTP（Bootstrap Protocol）

TCP/IPネットワークにおいて、クライアントがシステムの起動に必要なプログラムをサーバから自動的に取得するプロトコルです。
BOOTPサーバは、ネットワークに関連した情報（IPアドレス、デフォルト・ルータのIPアドレス、設定ファイルのファイル名）などを管理しています。BOOTPクライアントが起動すると、BOOTPサーバが自動的にIPアドレスを割り振ります。
BOOTPサーバはクライアントとIPアドレスを一元的に管理しています（1つのクライアントに1つのIPアドレスが対応)。そのため、割り当てることができるIPアドレスの数とクライアントの数を等しくする必要があります。
本製品のDHCP/BOOTPサーバ機能を使う場合、BOOTPサーバだけをサポートしているMacintoshのMacTCPでは、IPアドレスだけが割り当てられます。

CHAP（Challenge Handshake Authentication Protocol）

PPP接続で使用されるユーザ認証方法の1つです。最初にPPPサーバがChallenge Valueという乱数をPPPクライアントに送ります。PPPクライアントはその乱数を使ってパスワードを演算し、その結果をPPPサーバに返します。PPPサーバは受け取った値と自分で計算した値とを比較し、同じであれば接続を許可します。
Challenge Valueは認証のたびに変えるため、同じユーザー名とパスワードでも演算の結果は毎回異なります。したがって、たとえ通信回線を盗聴されても、不正利用される可能性は低くなります。ユーザ名とパスワードだけで単純に認証するPAPよりセキュリティの高い方法といえます。

DHCP（Dynamic Host Configuration Protocol）

TCP/IPネットワークにおいて、クライアントがシステムの起動に必要なプログラムをサーバから自動的に取得するプロトコルです。DHCPはBOOTPを拡張したプロトコルです。
DHCPサーバは、ネットワークに関連した情報（IPアドレス、デフォルト・ルータのIPアドレス、設定ファイルのファイル名、ドメイン名）などを管理しています。DHCPクライアントが起動すると、DHCPサーバが自動的にIPアドレスを割り振ります。
DHCPクライアントに割り当てるIPアドレスの有効期限を設定できます。有効期限を過ぎると割り当て済みのIPアドレスを再利用することができるので、効率よくIPアドレスを使用することができます。
本製品のDHCP/BOOTPサーバ機能を使う場合、DHCPサーバをサポートしているTCP/IPでは、IPアドレスのほかにデフォルト・ルータのIPアドレスなどが割り当てられます。

DHCP/BOOTPサーバ機能

→技術解説「DHCP/BOOTPサーバ機能」〈P.147〉

DNS（Domain Name System）

TCP/IPネットワークにおける名前解決サービスのことです。DNS（ドメイン・ネーム・システム）にしたがってドメインネームサーバにコンピュータ名やドメイン名を登録して、ドメインネームサービスを提供しています。ドメインネームサービスを利用すると、「192.168.0.1」などの分かりにくい数字ではなく、分かりやすいドメイン名やホスト名で目的のサイトを指定することができます。

DMZ（DeMilitarized Zone）

LAN側のネットワークとインターネットとの間に、ルータを介して設けられる区域のことです。
インターネットにWebサーバなどを公開することによってLAN型で接続している端末に、インターネットから不正な接続がされる可能性を減らすために、サーバをこの区域に設定します。

FTP（File Transfer Protocol）

TCP/IPネットワークでファイルを転送するためのプロトコル、またはそのサービスを指します。FTPはおもに、ホストから自分のコンピュータへのファイル転送に使われます。インターネット上に多数存在するFTPサーバから、フリーウェアやシェアウェア、サウンドや画像のデータをダウンロードしたり、自作のプログラムやデータをFTPサーバへアップロードして公開しています。

IP（Internet Protocol）

TCP/IPネットワークにおけるネットワーク層プロトコルです。ネットワーク内またはネットワーク間のデータパケット送受信を制御するコネクションレス型プロトコルです。

IPCP（Internet Protocol Control Protocol）

PPPは主に、LCPとNCP（Network Control Protocol）の2種類のプロトコルで構成されています。NCPは、ネットワーク層プロトコルをPPP環境で使用するための制御機能を実現します。NCPはネットワーク層プロトコルごとに規定する必要があり、IP用に規定されているのがIPCPです。クライアントへIPアドレスを割り当てたりします。

IP Masquerade

→技術解説「IP Masquerade」〈P.149〉

IPsec（Security Architecture for Internet Protocol）

→技術解説「IPsec」〈P.153〉

IPフィルタ

→「フィルタ」〈P.157〉

L2TP（Layer2 Tunneling Protocol）

→技術解説「L2TP」〈P.153〉

LAN型ダイヤルアップ接続

LANとLANを電話回線を介して接続するための契約です。この契約をしたときは、LANの規模に応じたIPアドレスがプロバイダから指定され、そのIPアドレスを設定してプロバイダに接続します。

MACアドレス

ネットワーク上の個々の端末を区別するための物理アドレスです。すべてのEthernetカードには固有のアドレスが割り当てられていて、これを元にデータの送受信が行われます。アドレスはIEEE（アメリカ電気電子学会）によって世界的に管理されています。
MACアドレスの確認方法は、「パソコンのMACアドレスを確認する」〈P.25〉を参照してください。

MP（PPP Multilink Protocol）

ISDN回線で高速通信を実現する方法の１つで、複数のチャネルを使用してPPP通信する方式のことです。INSネット64の2つのBチャネルを同時に接続すると、128kbpsの通信速度が可能になります。

MPPE（Microsoft Point to Point Encryption）

PPPでのダイヤルアップ接続、またはPPTP VPN接続のデータを暗号化する方法で、本製品ではMPPEでは暗号化アルゴリズムとしてRC4を使用し、鍵長は40bitと128bitをサポートしています。なお、MPPEには、MS-CHAPによって生成された共通のクライアントキーとサーバキーが必要です。

MSS（Maximum Segment Size）

TCP接続をする際に、1つのTCPパケットとして受信できるデータサイズの最大値を、相手先に通知するためのTCPのオプションです。

MTU（Max Transfer Unit）

TCP/IPのパケットサイズの最大値を決めるパラメータのことです。

OCN（Open Computer Network）

NTTが提供するデータ通信用の回線サービスのことです。インターネットで使用されているTCP/IPを基調にしていて、インターネットにも接続されています。OCNのサービスには、インターネットへ常時接続する「OCN常時接続サービス」と、必要なときに電話をかけて接続する「OCNダイヤルアクセスサービス」があります。

OCNエコノミーサービス

OCN常時接続サービスのうち、もっとも低料金のサービスです。OCNエコノミーサービスを契約すると、アクセス時間や電話料金を気にせず、インターネットを利用できます。本製品では、OCN常時接続サービスのうち、このOCNエコノミーサービスのみ使用できます。

PPTP（Point to Point Tunneling Protocol）

→技術解説「PPTP」〈P.153〉

Super G
米アセロス・コミュニケーションズ社の開発した、無線欄のスループットを向上させる技術です。同社の独自技術である、「パケットバースト転送」「動的な転送最適化」「データ圧縮機能」を組み合わせることで、実効スループットを大幅に向上しています。

UPnP（Universal Plug and Play）
インターネットで標準になっている技術を元にして、家庭内にあるパソコンやAV機器、電話、家電製品などをネットワークにつなぐだけで利用可能にすることを目指した技術です。本製品はこの技術に対応しており、同じくUPnPに対応したアプリケーションソフトである「Windows Messenger」や「MSN Messenger」を利用して、複雑な設定なしにインターネット上での通話を行うことができます。

VPN（Virtual Private Network）
→技術解説「VPN」〈P.152〉

WINS（Windows Internet Name Service）
Windowsのコンピュータ名とIPアドレスを結びつける名前解決サービスの１つです。
WINSクライアントは起動するとWINSサーバにコンピュータ名とIPアドレスを登録し、WINSサーバは定期的に各サブネットのコンピュータ名とIPアドレスの情報を交換します。WINSクライアントは、WINSサーバからサブネットをまたがる他のWINSクライアントのコンピュータ名とIPアドレスの情報を取得することができます。

WEP（Wired Equivalent Privacy）
無線LANの国際規格のIEEE802.11できめられている暗号化技術です。アクセスポイントと端末の両方で、同じ文字列からなる「キー（鍵）」を設定しておき、そのキーを使ってデータの暗号化や復号化が行われます。

WPA-PSK
WPA（Wi-Fi Protected Access）とは、Wi-Fi Allianceが提唱する認証と暗号化をあわせた最新のセキュリティ規格です。本製品では、Pre-Shared Key（WPA共有キー）を利用する「WPA-PSKモード」が利用できます。従来から利用されているWEPの弱点を克服した暗号化方式「TKIP」や、次世代の標準と言われる強力な暗号化方式「AES」を利用できるので、無線LANのセキュリティ強度を大幅に向上させることができます。

アクセスポイント
無線LANカードを装着したパソコンと有線LANの通信を中継したり、無線LANカードを装着したパソコン同士の通信を中継する機器のことです。

グローバル着信
INSネット64でダイヤルインサービスを使用しているときに、契約者回線番号側への着番号の通知を省略するどうかを指定する機能です。INSネット64の契約時に「グローバル着信あり」にすると、相手側から契約者回線番号で着信要求があったとき、通信できるすべての機器が着信します。このとき、本製品でグローバル着信の設定を行うと、特定の機器にのみ着信させることが可能になります。

サブネットアドレス通知サービス
INSネット64の基本サービスの1つです。使用しているISDN回線に複数のISDN機器がつながっている場合に、それぞれの機器にサブアドレスを付けることができます。このサービスを利用すると、相手がこちらに接続するときに、回線番号に加えてサブアドレスを指定することにより、特定の機器を直接指定することができるようになります。

サブネット/サブネットマスク
32ビットで構成されるIPアドレスは、クラスに応じてネットワーク番号とホスト番号に分けられます。ネットワーク番号は、固有のネットワークに割り当てられ、各ホストにはホスト番号を割り当てます。このとき、サブネットマスクを指定すると、ネットワークの中でさらにサブネットを指定することができ、ネットワーク構築の自由度が上がります。サブネットマスクは、32ビットのうちサブネットとして指定したい部分を１で表し、「11111111.11111111.11111111.00000000」などのように設定しますが、通常10進数で「255.255.255.0」と表します。

スイッチングハブ
パソコンなどの端末から送られてきたデータをMACアドレスをベースに解析し、送り先の端末だけにデータを送信する機能を搭載しているハブのことです。

スタティックルーティング
ユーザがあらかじめ中継経路（ルーティングテーブル）を固定的に設定する方式のことです。

スタティックルート
ユーザがあらかじめ決めた中継経路のことです。

ステートフル・パケット・インスペクション（SPI）
ファイヤーウォールを通過するパケットのデータを読み取って内容を判断し、動的にポートを開放したり閉鎖したりする機能です。

ステルスモード
インターネット側から送信されるPingコマンド（ポート打診）に応答せず、またICMPエラーやTCPリセットを返さなくなる機能です。外部からの不正侵入のために行われることもある外部からのポートスキャンに反応しないので、インターネット上で本製品の存在を隠すことができます。

セッション
ネットワーク上の2つのホスト間の通信のことです。個々のホストは、同時に複数のセッションを行うことができます。

ダイナミックルーティング
ルータ同士で経路情報やトラフィック情報をやりとりすることによって、中継するルータの数や遅延時間が最小になる最適な経路を自動的に選択して、パケットを転送する方式のことです。

端末型ダイヤルアップ
１台のパソコンでインターネットを利用するための契約です。この契約をしたときはプロバイダに接続したときに、そのパソコンのIPアドレスが割り当てられます。
ただし、本製品ではLANにつながっているパソコンでも端末型ダイヤルアップ接続の契約でインターネットを利用できます。

デフォルトルータアドレス
→技術解説「デフォルトルータアドレス」〈P.146〉

デフォルトルート
パケットを送信するときに、そのアドレスがルーティングテーブル内に明示的に記載されていないときに使用される、デフォルトルータまでの経路のことです。

ドメイン名
インターネットに接続するコンピュータはIPアドレスと呼ばれる数字を使って識別されていますが、数字よりも簡単に覚えられるように考えられた文字で表現された名前のことです。
ドメイン名は、文字の並びであるラベル、あるいはピリオドで区切られた複数のラベルから構成されます。
例）株式会社エヌ・ティ・ティ エムイーのドメイン名
　　ntt-me.co.jp
上記の場合、ntt-me、co、jpの3つのラベルがあり、ドメイン名としてはntt-me.co.jp、co.jp、jpの3つのレベルのドメインから構成されます。

ドメイン名解決要求／解決応答
DNS（ドメインネームシステム）サーバには、ドメイン名と対応するIPアドレスが登録されています。通信したい相手のIPアドレスがわからない場合、DNSサーバにドメイン名を問い合わせると、そのドメイン名に対応するIPアドレスが通知されます。

ニーモニック
複雑な情報や長い情報を、簡単で覚えやすいものと結びつけるのに使用される単語など、記憶の助けになるものを指します。

パケット
ネットワーク上を流れるデータの単位で、制御信号からなるヘッダと情報データを含むビット列のことです。ヘッダには宛先アドレスや送信元アドレス、データの内容を表わすフラグなどが記録されており、プロトコルや通信方法によって多様です。

ハブ
LANを拡大するためのハードウェアです。ハブには複数のポートがついていて、各ポートにパソコン、ワークステーション、サーバなどを接続できます。
ハブにルーティング、ネットワーク管理などの機能が追加され、ネットワークの中心となっているものもあります。
LANを構築する場合、10/100BASE-Tケーブルを使用するときは、ハブが必要になります。

ファイアウォール
内部のネットワークへ、外部から侵入されることを防ぐシステムです。内部のネットワークと外部のネットワークの境界でデータを監視し、不正なアクセスを検出したり遮断したりします。このシステムが組み込まれたコンピュータ自身をさして「ファイアウォール」と呼ぶこともあります。

フィルタ
通過しようとするデータになんらかの処理を施すものです。アドレスを元に、通すパケットと通さないパケットを判別するために使用します。

フィルタリング
通すべきでないデータを遮断することです。
トラフィックの増大を防いだり、不正なアクセスを防いだりします。

ブロードキャスト
同一のネットワーク内のすべてのハードウェアへパケットを送信すること（同報通信）です。

ブロードキャストアドレス

→技術解説「ブロードキャストアドレス」〈P.146〉

ブロードバンド

xDSL、CATV、光ファイバーなど、帯域幅が広く転送能力が高い通信方式の総称です。

ホスト

インターネットでは、WWWサーバやメールサーバなどの各種サービスを行うコンピュータをホストとして扱います。

ポート番号

通信を行うアプリケーションとTCPまたはUDPを対応付ける番号のことです。

ホップカウント

パケットが伝送されている間に通ったルータの数を指します。RIPではホップカウントを16に制限しています。

リセット（RST）パケット

このパケットは、再送信などの通常の方法で回復できないエラーが発生した場合や、サーバがシステムダウンした場合に使われます。

リモートアクセス

公衆電話回線などを使用して、遠隔地のパソコンからLANなどのネットワークに接続することです。LANにリモートアクセスすると、LANに直接つながっているパソコンと同様に、データ共有、プリンタ共有などLANの資源を使用することができます。

リモートアクセスIPクライアント

PPPソフトを使用して、遠隔地のパソコンから電話回線を介してTCP/IPのLANに接続するユーザのことを指します。

索引

MN128-SOHO IB3　活用ガイド～中・上級編

発行日：2004年6月　　第2版

発　行：株式会社エヌ・ティ・ティ エムイー

URL　http://www.ntt-me.co.jp/